THE ANALYTIC REPRESENTATION OF SUBSTITUTIONS ON A POWER OF A PRIME NUMBER OF LETTERS WITH A DISCUSSION OF THE LINEAR GROUP.

[CONTINUED.]

By Dr. Leonard Eugene Dickson, Chicago, Ill.

PART II.—Linear Groups.

Section I.—*Linear Homogeneous Group.*

1. We may define p^{nm} letters

$$l_{\xi_1, \xi_2, \ldots, \xi_m}$$

characterized by m indices, each being an arbitrary mark of the Galois field of order p^n. The general *linear homogeneous substitution* A on these letters replaces $l_{\xi_1, \ldots, \xi_m}$ by $l_{\xi'_1, \ldots, \xi'_m}$, where

$$\xi'_i = \sum_{j=1}^{m} a_{ij}\xi_j \qquad (i = 1, 2, \ldots, m) \quad (1)$$

where the a_{ij}'s are marks of the $GF[p^n]$. But (1) will indeed be a substitution on the p^{nm} letters if and only if the determinant

$$|A| \equiv |a_{ij}| \neq 0 . \qquad (i, j = 1, 2, \ldots, m)$$

For there must be one and only one system of m indices ξ_i which (1) replaces by a given system ξ'_i and hence an unique set of values ξ_j satisfying the equations

$$\sum_{j=1}^{m} a_{ij}\xi_j = \xi'_i . \qquad (i = 1, \ldots, m)$$

Remark. If the substitution (1) be identical with

$$\xi'_i = \sum_{j=1}^{m} \bar{a}_{ij}\xi_j \qquad (i = 1, \ldots, m)$$

then must

$$\bar{a}_{ij} = a_{ij} . \qquad (i, j = 1, 2, \ldots, m)$$

This follows if we take in turn, for $j = 1, 2, \ldots m$, the particular set of values

$$\xi_j = 1 ; \ \xi_i = 0 . \qquad (i = 1, 2, \ldots, m ; \ i \neq j)$$

PART II.—LINEAR GROUP.

SECTION I.—*Linear homogeneous group.*

SECTION II.—*Linear fractional group.*

SECTION III.—*The Betti-Mathieu group.*

PREFACE.

This paper is an application of the Galois Field theory, a conception of fundamental importance in Higher Algebra. This theory is here presupposed and will be used in the abstract form given it by E. H. Moore.[1] Reference may also be made to Galois,[2] Serret[3], Jordan[4], Borel et Drach[5], in a note by the latter the Galois Field being developed in its abstract form.

The aim in Part I is two-fold: (1) the complete determination of all quantics up to as high a degree as practicable which are suitable to represent substitutions on p^n letters, p being a prime, n an integer; (2) the determination of special quantics suitable on p^n letters, where for each quantic the combination (p, n) takes infinitely many values.

It is a remarkable fact that, on the one hand, the conditions necessary and sufficient to determine a substitution quantic are found by multinomial expansions,—on the other hand, one of the observed types of substitution quantics having an infinite range of suitability is a multinomial expansion

[1] Moore, *Proceedings of the Congress of Mathematics of* 1893, *at Chicago*.

[2] Galois, *Bulletin des Sciences mathématiques* de M. Férussac, vol. 13, p. 428, 1830; reprinted in Liouville's *Journal de Mathématiques*, vol. 11, pp. 398–407, 1846.

[3] Serret, *Algèbre supérieure*, fifth edition, vol. 2, pp. 122–189.

[4] Jordan, *Traité des substitutions*, pp. 14–18.

[5] Borel et Drach, *Théorie des Nombres et Algèbre supérieure*, 1895, pp. 42–50, 58–62; Note, pp. 343–350.

(multiplied by a power of the variable) and the other type a reverse-binomial expansion (see §§ 53–54).

The results of this investigation warrant the conjecture that there exist a small number of types of substitution quantics of such wide ranges that together they represent all the $p^n!$ substitutions on p^n letters. Examples where apparently isolated quantics fall under a general type (when it is not *reduced*) are given in § 77.

While the aim in Part II* is primarily to generalize the work of Jordan on the linear homogeneous group, the treatment has been considerably modified to render the subject more accessible. The desire being chiefly non-cyclic simple groups, the modulus is supposed prime, which affords much simplification. On the other hand, many amplifications occur and also the correction of several errors (indicated by foot-notes).

In the same investigation there may occur marks of the Galois Fields of orders p^1, p^n, amd p^{mn}, $n > 1$, $m > 1$, when (as a useful notation) we use small Roman, small Greek, and capital Roman letters respectively.

Literature on the analytic representation of substitutions:

M. Hermite, *Sur les fonctions de sept lettres, Comptes Rendus des Séances de L'Académie des Sciences*, vol. 57, pp. 750–757, 1863.

Hermite's results (in whole or part) are given by:

Serret, *Cours D'Algèbre supérieure*, vol. 2, pp. 383–389 and 405–412;

Netto, *Substitutionentheorie*, ch. 8;

Jordan, *Traité des Substitutions*, pp. 88–91;

Borel et Drach, *Théorie des Nombres et Algèbre supérieure*, pp. 305–307, 1895.

Enrico Betti, *Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo, Annali di Scienze Matematiche e Fisiche*, vol. 2, pp. 5–19, 1851; *Sulla risoluzione delle Equazioni algebriche*, ibid, vol, 3, pp. 49–115, 1852; *Sopra la teorica delle sostituzioni*, ibid, vol. 6, pp. 5–34, 1855.

Émile Mathieu, *Mémoire sur le nombre de valeurs que peut acquérir une fonction quand on y permute ses variables de toutes les manières possibles*, Journal de Mathématiques *pure et appliquées*, second series, vol. 5, pp. 9–42, 1860; *Mémoire sur l'etude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables*, ibid, vol. 6, pp. 241–323, 1861.

F. Brioschi. *Des substitutions de la forme*

$$\theta(r) = e(r^{n-2} + ar^{\frac{n-3}{2}})$$

* For the suggestion of this generalization as leading to a triply infinite system of simple groups, as also for much valuable aid throughout the investigation, I am indebted to Professor Moore.

pour un nombre n premier de lettres, *Mathematische Annalen*, vol. 2, pp. 467–470, 1870.

De Polignac, *Sur la représentation analytique des substitutions*, *Bulletin de la Société Mathématique de France*, vol. 9, pp. 59–67, 1881.

A. Grandi, *Un teorema sulla rappresentazione analitica delle sostituzioni sopra un numero primo di elementi*, *Giornale Matematico* del Prof. G. Battaglini, vol. 19, pp. 238–245. The conditions are found under which

$$x^{p-s} + ax^{\frac{p+s+1}{2}} + bx$$

shall represent a substitution on p letters. A generalization by the same writer is given in *Reale Istituto Lombardo di scienze e lettere*, *Rendiconti*, Milano, vol. 16, pp. 101–111. For abstracts of each see *Fortschritte der Mathematik*, vol. 13, p. 118, 1881, and vol. 15, p. 116, 1883.

J. L. Rogers, *On the Analytical Representation of Heptagrams*, *London Mathematical Society*, vol. 22, pp. 37–52, 1890.

L. E. Dickson, *Analytic Functions Suitable to Represent Substitutions*, *American Journal of Mathematics*, vol. 18, pp. 210–218, 1896.

PART I.—Analytic Representation of Substitutions on a Power of a Prime Number of Letters.

Section I.—*General Theory.*

1. Let ξ be any mark of the Galois Field of order p^n, p being a prime and n a positive integer. Also let $\varphi(\xi)$ be an integral function of ξ having as coefficients certain marks of the $GF[p^n]$. The replacing of the letter l_ξ by the letter $l_{\phi(\xi)}$ defines a *substitution* on p^n letters, in notation,

$$\xi' = \varphi(\xi).$$

2. In order that $\varphi(\xi)$ shall indeed be suitable to represent a substitution on the marks

$$\mu_i \qquad (i = 0, 1, \ldots, p^n - 1),$$

it is necessary and sufficient that $\varphi(\mu_0)$, $\varphi(\mu_1)$, $\ldots$, $\varphi(\mu_{p^n-1})$, be identical with $\mu_0, \mu_1, \ldots, \mu_{p^n-1}$, except as to order. If an integral function of degree k belonging to the $GF[p^n]$ satisfies these conditions, it will be called a *substitution quantic* of degree k on p^n letters and denoted thus

$$SQ[k; p^n].$$

The degree k will be supposed $< p^n$ owing to the equation

$$\xi^{p^n} = \xi ,$$

satisfied by every mark of the field.

3. Theorem. *Two different quantics $\varphi(\xi)$ and $\psi(\xi)$ belonging to the $GF[p^n]$ cannot represent the same literal substitution.*

For if the substitution replace the index μ_i by μ_{a_i} for $i = 0, 1, \ldots, p^n - 1$, then must

$$\varphi(\mu_i) = \mu_{a_i} = \psi(\mu_i) \qquad (i = 0, 1, \ldots, p^n - 1).$$

Thus

$$\varphi(\xi) - \psi(\xi) = 0$$

is of degree $p^n - 1$ at most but has p^n distinct roots μ_i. It is thus an identity in ξ.

4. The most evident substitution quantic is the integral function $\varphi(\xi)$ which gives Lagrange's interpolation formula:

$$\varphi(\xi) \equiv \sum_{i=0}^{p^n-1} \frac{\mu_{a_i} F(\xi)}{(\xi - \mu_i) F'(\mu_i)} \tag{1}$$

where $a_0, a_1, \ldots, a_{p^n-1}$ is any permutation of $0, 1, \ldots, p^n - 1$, and where

$$F(\xi) \equiv \prod_{i=0}^{p^n-1} (\xi - \mu_i) ,$$

and F' denotes its derivative. Thus

$$\xi' = \varphi(\xi)$$

represents the substitution

$$\begin{pmatrix} \mu_0 , & \mu_1 , & \ldots , & \mu_{p^n-1} \\ \mu_{a_0} , & \mu_{a_1} , & \ldots , & \mu_{a_{p^n-1}} \end{pmatrix} .$$

5. Following Hermite's method* for the case $n = 1$, we may give (1) a simpler form.

In the $GF[p^n]$,

$$F(\xi) = \xi^{p^n} - \xi ; \quad F'(\xi) = -1 .$$

$$\varphi(\xi) \equiv -\sum_{i=0}^{p^n-1} \frac{\mu_{a_i} (\xi^{p^n} - \xi)}{\xi - \mu_i} .$$

Taking $\mu_0 = 0$, so that

$$\mu_i^{p^n-1} - 1 = 0 \qquad (i = 1, 2, \ldots, p^n - 1)$$

* Cf. Serret, l. c. 2, pp. 384–5.

and performing the division by $\xi - \mu_i$,

$$\varphi(\xi) \equiv -\mu_{a_0}(\xi^{p^n-1} - 1) - \sum_{i=1}^{p^n-1} \mu_{a_i}(\xi^{p^n-1} + \mu_i \xi^{p^n-2} + \ldots + \mu_i^{p^n-2}\xi).$$

Arranging according to powers of ξ and noting that*

$$\mu_{a_0} = -\sum_{i=1}^{p^n-1} \mu_{a_i},$$

we reach the desired quantic,

$$\varphi(\xi) \equiv \sum_{j=0}^{p^n-2} a_j \xi^j \tag{2}$$

where

$$a_j = -\sum_{i=0}^{p^n-1} \mu_{a_i} \cdot \mu_i^{p^n-1-j} \quad (j = 0, 1, \ldots, p^n - 2). \tag{3}$$

It follows from § 3 that every substitution quantic on p^n letters which belongs to the $GF[p^n]$ is contained in the form (2).

6. The conditions on a_j that an arbitrary quantic

$$\varphi(\xi) \equiv \sum_{j=0}^{p^n-1} a_j \xi^j$$

belonging to the $GF[p^n]$ shall represent a substitution on its p^n marks μ_i are

$$\sum_{j=0}^{p^n-1} a_j \mu_i^j = \varphi(\mu_i) \qquad (i = 0, 1, \ldots, p^n - 1), \tag{4}$$

where $\varphi(\mu_i) \equiv \mu_{a_i}$ form a permutation of μ_i. Applying the lemma proven in § 10, we have on adding the p^n equations (4),

$$-a_{p^n-1} = \sum_{i=0}^{p^n-1} \varphi(\mu_i) = 0.$$

Taking a_{p^n-1} zero and dropping the first one of the equations (4), we have the system of conditions

$$\sum_{j=0}^{p^n-2} a_j \mu_i^j = \varphi(\mu_i) \qquad (i = 1, 2, \ldots, p^n - 1). \tag{4'}$$

The determinant†

$$|\mu_i^j| = \Pi(\mu_r - \mu_s) \neq 0,$$

where $r, s = 1, 2, \ldots, p^n - 1$, $r > s$.

We may thus express a_j linearly in terms of μ_{a_i}. By equation (2) of § 5, this is done by formula (3).

---

* $\sum_{i=0}^{p^n-1} \mu_{a_i} = \sum_{i=0}^{p^n-1} \mu_i = 0$ by § 10.

† Baltzer, *Theorie und Anwendung der Determinanten*, p. 85.

7. The gist of De Polignac's paper is to actually solve equations (4) for the case $n = 1$. Using a and m for the integers corresponding to the marks α and μ, his result is given in the form

$$a_j = \sum_{i=1}^{p-2} \{(-1)^j - i^{p-1-j}\}\, m_{a_i},$$

where previously m_{a_0} has been taken to be zero. Subtracting

$$(-1)^j \cdot \sum_{i=1}^{p-1} m_{a_i} \quad 0 \pmod{p},$$

$$a_j = -(-1)^j m_{a_{p-1}} - \sum_{i=1}^{p-2} i^{p-1-j} m_{a_i} = -\sum_{i=1}^{p-1} i^{p-1-j} m_{a_i}. \qquad (3_{n=1})$$

8. We may independently verify the inverse character of the linear relations (3) and (4) between the coefficients a_j of any substitution quantic $\varphi(\xi)$ and the marks $\varphi(\mu_i) = \mu_{a_i}$. By (4′) the matrix

$$\begin{pmatrix} 1, & \mu_1, & \mu_1^2, & \ldots, & \mu_1^{p^n-2} \\ 1, & \mu_2, & \mu_2^2, & \ldots, & \mu_2^{p^n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1, & \mu_{p^n-1}, & \mu_{p^n-1}^2, & \ldots, & \mu_{p^n-1}^{p^n-2} \end{pmatrix}$$

expresses $\varphi(\mu_1)$, $\varphi(\mu_2), \ldots, \varphi(\mu_{p^n-1})$ linearly in terms of $\alpha_0, \alpha_1, \ldots, \alpha_{p^n-2}$. Inversely, by (3) the matrix

$$\begin{pmatrix} -1, & -1, & \ldots, & -1 \\ -\mu_1^{p^n-2}, & -\mu_2^{p^n-2}, & \ldots, & -\mu_{p^n-1}^{p^n-2} \\ -\mu_1^{p^n-3}, & -\mu_2^{p^n-3}, & \ldots, & -\mu_{p^n-1}^{p^n-3} \\ \cdot & \cdot & \cdot & \cdot \\ -\mu_1, & -\mu_2, & \ldots, & -\mu_{p^n-1} \end{pmatrix}$$

expresses the latter linearly in terms of the former. To prove that the product of the two matrices is the identity, let c^{ij} denote the term in the product derived from the ith row of the first and the jth column of the second matrix. Then

$$c_{ij} = -1 - \mu_i\mu_j^{p^n-2} - \mu_i^2\mu_j^{p^n-3} - \ldots - \mu_i^{p^n-2}\mu_j.$$

Thus

$$c_{ii} = -(p^n - 1) = +1 \qquad (i = 1, 2, \ldots, p^n - 1).$$

For $i, j = 1, 2, \ldots, p^n - 1$, but $i \neq j$,

$$1 = \frac{\mu_i^{p^n} - \mu_j^{p^n}}{\mu_i - \mu_j} = \mu_i^{p^n-1} + \mu_i^{p^n-2}\mu_j + \ldots + \mu_i\mu_j^{p^n-2} + \mu_j^{p^n-1}.$$

Hence $c_{ij} = 0$ if $i \neq j$.

From the matrix expressing $\varphi(\mu_i)$ in terms of $\alpha_0, \alpha_1, \ldots, \alpha_{p^n-2}$, we derive by reflection on its main diagonal and change of sign of all its elements a matrix which expresses $\alpha_0, \alpha_{p^n-2}, \alpha_{p^n-3}, \ldots, \alpha_1$ in terms of

$$\varphi(\mu_i) \qquad (i = 1, 2, \ldots, p^n - 1).$$

9. Lemma. $\mu_0, \mu_1, \ldots, \mu_{p^n-1}$, being the marks of the $GF[p^n]$ and t a positive integer,

$$\sum_{i=0}^{p^n-1} \mu_i^t = \begin{cases} 0 \text{ for } t < p^n - 1 \\ -1 \text{ for } t = p^n - 1 \end{cases}$$

For let σ_t denote the sum of the tth powers of the roots of the equation belonging to the $GF[p^n]$

$$\sum_{i=0}^{p^n} y_i \xi^{p^n-i} = 0 \qquad (y_0 = 1). \tag{5}$$

Applying Newton's identity (as is allowable)

$$\sigma_k + y_1\sigma_{k-1} + y_2\sigma_{k-2} + \ldots + y_{k-1}\sigma_1 + ky_k = 0. \quad (k = 1, \ldots, p^n)$$

If for (5) we take the equation whose roots are μ_i,

$$\xi^{p^n} - \xi = 0$$

the proof of the lemma follows.

10. Lemma. If, in the notation of § 9,

$$\sigma_{p^n-1} \neq 0, \ \sigma_t = 0 \quad \begin{Bmatrix} t = 1, 2, \ldots, p^n - 2 \\ t \not\equiv 0 \pmod{p} \end{Bmatrix},$$

and if all the roots of equation (5) be marks of the $GF[p^n]$, then will (5) take the form

$$\xi^{p^n} + y_{p^n-1}\xi + y_{p^n} = 0.$$

Applying Newton's identity cited above, we find

$$y_i = 0 \quad \begin{Bmatrix} i = 1, 2, \ldots, p^n - 2 \\ i \not\equiv 0 \pmod{p} \end{Bmatrix},$$

$$\sigma_p = \sigma_{2p} = \ldots = \sigma_{p^n-p} = \sigma_{p^n} = 0.$$

To determine $y_p, y_{2p}, \ldots, y_{p^n-p}$, apply the identity

$$\sigma_k + y_1\sigma_{k-1} + y_2\sigma_{k-2} + \ldots + y_{p^n}\sigma_{k-p^n} = 0 \qquad (k \leqq p^n),$$

which reduces to

$$\sigma_k + y_p\sigma_{k-p} + y_{2p}\sigma_{k-2p} + \ldots + y_{p^n-1}\sigma_{k-p^n+1} + y_{p^n}\sigma_{k-p^n} = 0 .$$

By our assumption on the roots,

$$\sigma_t = \sigma_{t+p^{n-1}} .$$

Hence for $k = p_n + p - 1$,

$$y_p\sigma_{p^n-1} = 0 .$$

Generally, for $k = p^n + lp - 1$, $l \leqq p^{n-1} - 1$,

$$yl_p\,\sigma_{p^n-1} = 0 .$$

Since $\sigma_{p^n-1} \neq 0$ by hypothesis, $y_{lp} = 0$.

11. *Generalization of Hermite's Theorem.*

The necessary and sufficient conditions that $\varphi(\xi)$ shall be suitable to represent a substitution on p^n letters are :

(1) *Every tth power of $\varphi(\xi)$, for $t < p^n - 1$ and prime to p, shall reduce to a degree $\leqq p^n - 2$ when we lower the exponents of ξ below p^n by means of the equation*

$$\xi^{p^n} - \xi = 0 ;$$

(2) *There shall be but one distinct root of*

$$\varphi(\xi) = 0 .$$

Proof : Suppose

$$\varphi(\xi) \equiv \sum_{i=0}^{p^n-1}{}' \alpha_i\xi^i .$$

After reducing exponents below p^n let

$$[\varphi(\xi)]^m \equiv \sum_{i=0}^{p^n-1}{}' \alpha_i^{(m)}\xi^i .$$

Give to ξ the values of the p^n marks μ_j of the field and add the resulting equalities.

$$\sum_{j=0}^{p^n-1}{}' [\varphi(\mu_j)]^m = p^n\alpha_0^{(m)} + \alpha_1^{(m)} \sum_{j=0}^{p^n-1}{}' \mu_j + \ldots + \alpha_{p^n-1}^{(m)} \sum' \mu_j^{p^n-1} .$$

Hence by § 9, for $m < p^n - 1$,

$$\sum_{j=0}^{p^n-1}{}' [\varphi(\mu_j)]^m = -\alpha_{p^n-1}^{(m)} .$$

But if $\varphi(\xi)$ represents a substitution,

$$\sum_{j=0}^{p^n-1}{}' [\varphi(\mu_j)]^m = \sum_{j=0}^{p^n-1}{}' \mu_j^m = 0$$

if $m < p^n - 1$. Hence a necessary condition is

$$a_{p^n-1}^{(m)} = 0 . \qquad (m = 1, 2, \ldots, p^n - 2)$$

Also there must be one and only one of the marks $\varphi(\mu_j)$ equal to zero, i. e. but one distinct root of $\varphi(\xi) = 0$.

Inversely, suppose (1) and (2) are satisfied, so that

$$\sum_{j=0}^{p^n-1}{}' [\varphi(\mu_j)]^t = -a_{p^n-1}^{(t)} = 0 \qquad \begin{pmatrix} t = 1, 2, \ldots, p^n - 2 \\ t \not\equiv 0 \pmod{p} \end{pmatrix}$$

$$\sum_{j=0}^{p^n-1}{}' [\varphi(\mu_j)]^{p^n-1} = -1 \not\equiv 0 .$$

Then by § 10 the equation

$$\prod_{j=0}^{p^n-1}{}' [\eta - \varphi(\mu_j)] = 0$$

takes the form

$$\eta^{p^n} + y_{p^n-1}\eta + y_{p^n} = 0$$

or

$$\eta(1 + y_{p^n-1}) + y_{p^n} = 0 .$$

If $y_{p^n-1} \neq -1$, this linear equation is satisfied by the p^n marks $\varphi(\mu_j)$. These must therefore be equal, and since their sum is zero, each must be zero. But in this case the equation belonging to our field,

$$\varphi(\xi) \equiv \sum_{i=0}^{p^n-2}{}' a_i \xi^i = 0$$

would have p^n distinct roots $\xi = \mu_i$ $(i = 0, 1, \ldots, p^n - 1)$ which is impossible. Hence $y_{p^n-1} = -1$ and then, since one of the $\varphi(\mu_j)$'s are zero, $y_{p^n} = 0$. Thus the marks $\varphi(\mu_j)$ are identical apart from order to the roots μ_i of

$$\eta^{p^n} - \eta = 0 .$$

12. Reciprocal* of a substitution quantic. Given a substitution quantic

$$\eta \equiv \varphi(\xi) \equiv \sum_{i=1}^{p^n-2}{}' a_i \xi^{p^n-1-i} .$$

* Rogers, l. c. for $p^n = 7$. His proof is objectionable, since he makes $\xi^6 \equiv 1 \pmod 7$ while ξ is to be taken $= 0$.

Suppose its reciprocal is

$$\xi = \sum_{t=1}^{p^n-2} \beta_t \eta^{p^n-1-t}.$$

Then

$$\xi\eta^t = \xi\,[\varphi(\xi)]^t \equiv \sum_{t=1}^{p^n-1} a_t^{(t)} \xi^{p^n-t},$$

after reduction of exponents as in § 11. On the other hand,

$$\xi\eta^t = \sum_{t=1}^{p^n-2} \beta_t \eta^{p^n-1-t+t} \equiv \beta_1\eta^{t-1} + \beta_2\eta^{t-2} + \ldots + \beta_t\eta^{p^n-1} + \ldots + \beta_{p^n-2}\eta^{t+1}.$$

Since $\eta \equiv \varphi(\xi)$ is a $SQ[\ ; p^n]$, then η^j contains no term ξ^{p^n-1} as long as $j < p^n - 1$. Hence the term $a_1^{(t)}\xi^{p^n-1}$ must be derived from $\beta_t\eta^{p^n-1}$. But $\eta = 0$ if and only if $\xi = 0$, so that $\eta^{p^n-1} = \xi^{p^n-1}$. Hence

$$\beta_t = a_1^{(t)}$$

or β_t is the coefficient of ξ^{p^n-2} in $[\varphi(\xi)]^t$.

Residue of a multinomial coefficient modulo p, p being prime, §§ 13–15.

13. A number m can be written in one and but one way in the form

$$m = \sum_{i=0}^{n} a_i^{(m)} p^i,$$

where $a_i^{(m)}$ is zero or a positive integer $< p$. Then,* if P_m denotes the highest power of p which divides $m!$, we have

$$P_m = (m - \sum_{i=0}^{n} a_i^{(m)})/(p-1).$$

14. Theorem. The multinomial coefficient

$$\frac{m!}{m_1!\, m_2! \ldots m_t!},$$

where $m_1 + m_2 + \ldots + m_t = m$, is prime to p if and only if, when each m_k is written in the form

$$m_k = \sum_{i=0}^{n} a_i^{(m_k)} p^i,$$

we have as numerical equalities

$$\sum_{k=1}^{t} a_i^{(m_k)} = a_i^{(m)} \qquad (i = 0, 1, \ldots, n).$$

* Bachmann, *Zahlentheorie*, I, p. 33.

Proof.—The necessary and sufficient condition is

$$P_m = P_{m_1} + P_{m_2} + \ldots + P_{m_t},$$

or

$$\sum_{i=0}^{n} a_i^{(m)} = \sum_{i=0}^{n} a_i^{(m_1)} + \sum_{i=0}^{n} a_i^{(m_2)} + \ldots + \sum_{i=0}^{n} a_i^{(m_t)}.$$

It follows that if m (written in the above form) be partitioned into $m_1 + m_2 + \ldots + m_t$, the partitioning must take place in the coefficients $a_i^{(m)}$ of the powers of p each independently of the others.

Example. $42 = 2^5 + 2^3 + 2$; hence the binomial coefficient c_k^{42} is *odd* only if $k = 2, 2^3, 2 + 2^3, 2^5, 2 + 2^5, 2^3 + 2^5, 2 + 2^3 + 2^5$.

15. Theorem. If the multinomial coefficient be prime to p, it is congruent modulo p to

$$\prod_i \frac{a_i^{(m)}!}{a_i^{(m_1)}!\, a_i^{(m_2)}! \ldots a_i^{(m_t)}!}$$

where $s! = 1$, if $s = 0$.

In proof let

$$m = pq_1 + r_1,\ q_1 = pq_2 + r_2,\ \text{etc.},$$

where $r_1, r_2, \ldots$ are positive integers $< p$. Then

$$m! = (1 \cdot 2 \cdot 3 \ldots \overline{p-1})\, p\, (\overline{p+1} \cdot \overline{p+2} \ldots \overline{2p-1})\, 2p \ldots q_1 p\, (\overline{q_1 p + 1} \ldots \overline{q_1 p + r_1})$$
$$\equiv (\overline{p-1}!)^{q_1} p^{q_1} \cdot q_1!\, r_1! \pmod{p}$$
$$\equiv (-p)^{q_1} \cdot q_1!\, r_1!.$$

Similarly,

$$q_1! \equiv (-p)^{q_2} \cdot q_2!\, r_2! \pmod{p}, \text{ etc.}$$

Hence

$$m! \equiv (-p)^{\Sigma q_i} \prod_i (r_i!).$$

But if $E(s)$ denotes the greatest integer in s,

$$\sum_i q_i = \sum_i E(n/p^i) = P_m.^*$$

Thus

$$m! = (-p)^{P_m} \prod_i a_i^{(m)}!$$

Proceeding likewise for $m_1!, m_2!, \ldots, m_t!$ and applying § 14, we have the proof of the theorem.

16. *Reduced form of substitution quantics.* Let $\varphi(\xi) = a_0\xi^k + a_1\xi^{k-1} + \ldots$ be a $SQ\,[k\,;\, p^n]$. If on the right and left of the substitution

$$\xi' = \varphi(\xi)$$

* Bachmann, *Zahlentheorie*, p. 32.

we apply linear substitutions of the form

$$\xi' = \beta_1\xi + \beta_2 \qquad (\beta_1 \neq 0)$$

we obtain a substitution

$$\xi' = \beta_1\varphi(\beta_1'\xi + \beta_2') + \beta_2 = \varphi_1(\xi).$$

Take $\beta_1' = 1$ and dispose of the indeterminate β_1 so that the coefficient of ξ^k in $\varphi_1(\xi)$ shall be unity. If $a_1 \neq 0$, the coefficient $k\beta_2' + \beta_1 a_1$ of ξ^{k-1} in $\varphi_1(\xi)$ can, by choice of β_2', be made zero, if and only if k be prime to p. Finally β_2 is chosen to make the constant term zero. Then $\varphi_1(\xi)$, in which the coefficient of ξ^k is unity, the constant term zero, and when k is prime to p the coefficient of ξ^{k-1} zero, will be called the *reduced form** of $\varphi(\xi)$ for the $GF[p^n]$.

17. Theorem. *$\xi^k + a_1\xi^{k-1} + a_2\xi^{k-2} + \ldots + a_{k-1}\xi$ is not a substitution quantic on p^n marks if p^n be of the form $mk + 1$, $k > 1$.* For on raising it to the power $(p^n - 1)/k$ the coefficient of ξ^{p^n-1} is $1 \neq 0$.

18. Theorem. *ξ^k is a $SQ[k; p^n]$ if and only if k be relatively prime to $p^n - 1$.*

For, l being any integer $< p^n - 1$ and prime to p, lk must not be a multiple of $p^n - 1$ (by § 11).

Corollary —The extraction of kth roots in the $GF[p^n]$ is *always* possible (and then uniquely) if and only if k be prime to $p^n - 1$.

SECTION II.—*Degree k prime to p.*

19. Using the same method as in my paper† giving a complete list of $SQ[k; p^1]$ for $k < 7$ and p any prime, I shall first determine all $SQ[k; p^n]$ for $k < 7$, p any prime not a divisor of k, and n any integer. After a preliminary study of septics, I shall conclude Section II with the derivation of a remarkable class of substitution quantics of arbitrary odd degree k.

Complete determination of reduced quantics of degree $k < 7$ suitable to represent substitutions on p^n letters, p being prime not a divisor of k, §§ 20–45.

20. ξ is suitable for every p^n.

21. ξ^2 is the reduced quadratic and is rejected by § 17 since p^n is odd.

22. $\xi^3 + a\xi$.

(a) The case p^n of the form $3m + 1$ is rejected by § 17.

(b) The case $p^n = 3m + 2$.

Then $(\xi^3 + a\xi)^{m+1}$ gives $(m + 1)a$ as the coefficient of ξ^{3m+1}. Hence, by

* By making use of the indeterminate β_1' a further reduction may often be made in $\varphi_1(\xi)$. The simplest form thus obtainable is called *ultimately reduced.* Thus $\xi^4 \pm 3\xi$ reduce to $\xi^4 + 3\xi$.

† *American Journal of Mathematics*, Vol. 18, pp. 210–218, 1896.

§ 11, $a = 0$; for if $m + 1$ were divisible by p, then would also $3m + 3$ or $p^n + 1$. The remaining form ξ^3 is suitable by § 18.

23. $\xi^4 + a\xi^2 + \beta\xi$.

The only case to consider here is $p^n = 4m + 3$.

The $m + 1$st power requires $(m + 1)\, a = 0$ or $a = 0$.

$(\xi^4 + \beta\xi)^{m+2}$ requires $\dfrac{(m + 2)(m + 1)}{2}\beta^2 = 0$, provided $p^n > 7$. Hence $\beta = 0$; for if $m + 2$ be divisible by p then is also $4m + 8$ or $p^n + 5$, i. e. $p = 5$, while p must be of the form $4l + 3$.

But ξ^4 is rejected by § 18, viz, by the power $l = 2m + 1$.

For the case above excluded, $p = 7$, $n = 1$, we have Hermite's result, the suitable quartics $\xi^4 \pm 3\xi$.

Reduced quintic $\xi^5 + a\xi^3 + \beta\xi^2 + \gamma\xi$, §§ 24–44.

24. The case $p^n = 5m + 2$. Hence n is odd.

The power $m + 1$ requires

$$(m + 1)\,\gamma + \frac{(m + 1)\,m}{2}\,a^2 = 0\,.$$

But $m + 1$ is divisible by p only if $p = 3$. Thus if $p \neq 3$,

$$5\gamma = a^2\,. \tag{1}$$

The power $m + 2$ requires if $p^n > 7$

$$\frac{(m + 2)(m + 1)\,m}{1\,.\,2\,.\,3}\{6a\beta\gamma + \beta^3 + (m - 1)\,a^3\beta\} = 0\,.$$

Hence if $p \neq 2$ and $p^n > 7$,

$$5\,(6a\beta\gamma + \beta^3) - 7a^3\beta = 0\,. \tag{2}$$

From (1) and (2), if $p \neq 2$ and $\neq 3$ and if $p^n \neq 7$,

$$5\beta^3 = a^3\beta\,. \tag{3}$$

The power $m + 3$ requires if $p^n > 7$

$$c_4^{m+3}\left\{4a\gamma^3 + 6\beta^2\gamma^2 + \frac{m - 1}{5}(10a^3\gamma^2 + 30a^2\beta^2\gamma + 5a\beta^4)\right.$$
$$\left. + \frac{(m - 1)(m - 2)}{5\,.\,6}(6a^5\gamma + 15a^4\beta^2) + \frac{(m - 1)(m - 2)(m - 3)}{5\,.\,6\,.\,7}\,a^7\right\} = 0\,.$$

Now $m + 3$ is divisible by p only if $p = 13$. Hence if p is neither 2 nor 13 we may divide off the binomial factor c_4^{m+3}. Multiplying the resulting equa-

tion by 5^4, replacing $5(m-1)$ by -7, etc., we have for p^n not 2^n, 7^1, 13^n the condition

$$20\alpha(5\gamma)^3 + 150\beta^2(5\gamma)^2 - 70\alpha^3(5\gamma)^2 - 1050\alpha^2\beta^2(5\gamma) - 875\alpha\beta^4 + 84\alpha^5(5\gamma) + 1050\alpha^4\beta^2 - 34\alpha^7 = 0. \quad (4)$$

Applying (1) to (4):

$$150\alpha^4\beta^2 - 875\alpha\beta^4 = 0,$$

from which by (3) we find $\beta = 0$.

For the proof that the resulting form

$$5\xi^5 + 5\alpha\xi^3 + \alpha^2\xi$$

does represent a substitution on $p^n = 5m \pm 2$ letters, α being arbitrary, see § 39.

25. The case $p^n = 13^n = 5m + 2$.

The powers $m+3$, $m+4$, $m+5$ give identities. The power $m+6$ requires

$$c_{14}^{m+6} \cdot 14\alpha^3\beta = 0 \text{ or } \alpha^3\beta = 0.$$

For, $5m + 2 \equiv 0 \pmod{13}$ i. e. $m \equiv 10 \pmod{13}$. Thus c_k^{m+6} or c_k^{13t+3} is $\neq 0$ only for $k = 1, 2, 3, 13, 14, 15, 16, 26, \ldots$, by § 14.

It follows from this equation and (3) that $\beta = 0$.

26. The case $p = 7$, $n = 1$.

Hermite gave the complete list of suitable forms:

$$\xi^5 \pm 2\xi^2.$$

$$\xi^5 + \alpha\xi^3 \pm \xi^2 + 3\alpha^2\xi, \ \alpha = \text{quadratic non-residue of } 7.$$

$$\xi^5 + \alpha\xi^3 + 3\alpha^2\xi, \ \alpha = \text{arbitrary}.$$

The last may be written $5\xi^5 + 5\alpha\xi^3 + \alpha^2\xi$.

27. The case $p^n = 3^n = 5m + 2$.

The powers $m+2$ and $m+3$ require by (2) and (4)

$$2\beta^3 = \alpha^3\beta \quad (2')$$

$$\alpha\gamma^3 - \alpha^3\gamma^2 + \alpha\beta^4 - \alpha^7 = 0. \quad (4')$$

Since $n \geqq 3$, $5m + 2 \equiv 0 \pmod{27}$ or $m \equiv 5 \pmod{27}$. Hence c_k^{m+6} or c_k^{27t+11} is $\neq 0$ only if $k = 1, 2, 9, 10, 11$, or $\geqq 27$.

The power $m+6$ thus requires, if $n > 3$,

$$c_{10}^{m+6} \cdot 10\alpha\beta^9 = \alpha\beta^9 = 0. \quad (5')$$

Thus $\beta = 0$ and (4′) becomes

$$\alpha(\gamma + \alpha^2)(\gamma^2 + \gamma\alpha^2 - \alpha^4) = 0 .$$

If $\alpha \neq 0$, $\gamma = -\alpha^2$; for if the last factor vanishes,

$$(\gamma + \alpha^2)^2 = -\gamma^2 ,$$

while -1 is a not-square in the $GF[3^1]$ and hence in the $GF[3^n]$, n being odd.

If $\alpha = 0$, the power $m + 9$ of $\xi^5 + \gamma\xi$ requires

$$c_{11}^{m+9}\gamma^{11} = \gamma^{11} = 0 .$$

The possible form is thus $5\xi^5 + 5\alpha\xi^3 + \alpha^2\xi$ when $n > 3$.

28. The case $p^n = 3^3$.

The powers 11 and 13 require

$$\beta + \alpha\beta^9 = 0 \tag{5″}$$

$$\beta^3\gamma + \beta\gamma^9 + \beta^9\gamma^3 + \beta^{13} = 0 . \tag{6″}$$

Suppose $\beta \neq 0$. Then by (2′), $\beta^2 = -\alpha^3$, so that (5′) is satisfied and (4′) becomes

$$\alpha\gamma^2(\gamma - \alpha^2) = 0 .$$

But if either $\gamma = 0$ or $\gamma = \alpha^2$, (6″) requires that $\beta = 0$. Since $\beta = 0$ we have $\gamma = -\alpha^2$ as in the case $n > 3$.

29. The case $p^n = 2^n = 5m + 2$.

Since $n \gtrless 5$, $m \equiv 6 \pmod{32}$. The power $m + 5$ requires

$$c_8^{m+5} \cdot \beta^8 + c_{10}^{m+5} \cdot 45\alpha^8\gamma^2 + c_{11}^{m+5}(11\alpha^{10}\gamma + 55\alpha^9\beta^2) = 0 .$$

Applying (1), $\gamma = \alpha^2$, this becomes

$$\beta^2(\beta^6 + \alpha^9) = 0 . \tag{7}$$

The power $m + 7$ requires if $n > 5$,

$$\alpha\gamma^8 + \alpha^5\beta^8 + \alpha^9\gamma^4 = 0 .$$

Applying (1) this becomes $\alpha^5\beta^8 = 0$. Hence $\beta = 0$.

For $n = 5$, the 13th power requires a condition which on applying (1) becomes exactly the fourth power of (7).

For $n = 5$, the 15th power requires

$$\gamma^{11} + \beta^4\gamma^8 + \alpha^4\gamma^9 + \beta^8\gamma^5 + \alpha^6\gamma^8 + \alpha^2\beta^8\gamma^4 + \beta^{12}\gamma^2 + \alpha^8\gamma^7 + \alpha^4\beta^8\gamma^3 + \alpha^2\beta^{12}\gamma + \alpha\beta^{14} = 0 .$$

Applying (1) this becomes

$$\alpha\beta^4 (\alpha^{15} + \alpha^9\beta^4 + \beta^{10}) = 0 . \tag{8}$$

If $\beta \neq 0$, $\beta^6 = \alpha^9$ by (7), whence (8) becomes $\alpha^{15} = 0$. Hence must $\beta = 0$.

30. Summary of §§ 24–29. The only possible reduced substitution quintic on $p^n = 5m + 2$ letters is

$$5\xi^5 + 5\alpha\xi^3 + \alpha^2\xi , \quad \alpha \text{ arbitrary},$$

except for $p = 7$, $n = 1$ when we have two additional forms:

$$\xi^5 \pm 2\xi^2$$

$$\xi^5 + \alpha\xi^3 \pm \xi^2 + 3\alpha^2\xi ,$$

where α is a quadratic non-residue of 7.

31. The case $p^n = 5m + 3$.

The power $m + 1$ requires $(m + 1)\beta = 0$. Hence if $p \neq 2$, $\beta = 0$. The power $m + 2$ of $\xi^5 + \alpha\xi^3 + \gamma\xi$ requires

$$c_2^{m+2}\gamma^2 + c_3^{m+2} \cdot 3\alpha^2\gamma + c_4^{m+2}\alpha^4 = 0 . \tag{1}$$

If $p \neq 7$ we may divide out c_2^{m+2}, giving readily

$$25\gamma^2 - 15\alpha^2\gamma + 2\alpha^4 = 0 .$$

Hence, if $p \neq 2, \neq 7$, either $5\gamma = \alpha^2$ or $5\gamma = 2\alpha^2$.

The power $m + 4$ requires for $p^n > 13$,

$$c_5^{5m+4} \cdot 5\alpha\gamma^4 + c_6^{m+4} \cdot 20\alpha^3\gamma^3 + c_7^{m+4} \cdot 21\alpha^5\gamma^2 + c_8^{m+4} \cdot 8\alpha^7\gamma + c_9^{m+4}\alpha^9 = 0 . \tag{2}$$

If p is not 2, 3, 7 or 17, we may divide out $(m + 4)(m + 3)(m + 2)(m + 1)m$, multiply by $5^4 \cdot 7!$ and replace $5(m - 1)$ by -8, etc., giving

$$210\alpha(5\gamma)^4 - 8 \cdot 140\alpha^3(5\gamma)^3 + 8 \cdot 13 \cdot 21\alpha^5(5\gamma)^2 - 8 \cdot 13 \cdot 18\alpha^7(5\gamma) + 23 \cdot 26\alpha^9 = 0 .$$

If $5\gamma = \alpha^2$, this becomes

$$\alpha^9 (210 - 8 \cdot 140 + 8 \cdot 13 \cdot 21 - 8 \cdot 13 \cdot 18 + 23 \cdot 26) = 0 ,$$

in which the coefficient of α^9 is identically zero. If $5\gamma = 2\alpha^2$, the coefficient of α^9 reduces to -10. Hence in this case $\alpha = \gamma = 0$.

Thus for p^n not 2^n, 3^n, 7^n, 17^n or 13, the only possible quintic on $p^n = 5m + 3$ letters is reducible to

$$5\xi^5 + 5\alpha\xi^3 + \alpha^2\xi .$$

32. For $p = 13$, $n = 1$, I have elsewhere* shown that the only suitable quintics are

$$5\xi^5 + 5a\xi^3 + a^2\xi, \quad a = \text{arbitrary}.$$
$$5\xi^5 + 5a\xi^3 + 2a^2\xi, \quad a = \text{quadratic non-residue of 13}.$$

33. The case $p^n = 17^n = 5m + 3$.

The value $5\gamma = 2a^2$ is rejected since the equation

$$5\xi^5 + 5a\xi^3 + 2a^2\xi = 0$$

has a solution $\neq 0$ for every a when $p = 17$. Thus

$$5\xi(\xi^4 + a\xi^2 - 3a^2) = 0$$

has the solutions $\xi^2 = 4a$ and $-5a$. Now -5 is a not-square in the $GF[17^1]$ and hence also in the $GF[17^n]$, n being odd. Thus whether a be a square or a not-square, we have a solution $\xi \neq 0$ belonging to the field.

34. The case $p^n = 7^n = 5m + 3$.

The condition (2) of § 31 becomes

$$5 \cdot 8 \cdot 9a^7\gamma - 23a^9 = 0.$$

Thus either $a = 0$ or $\gamma = 3a^2$.

But the power $m + 6$ of $\xi^5 + \gamma\xi$ requires $\gamma^7 = 0$.

The only possible form is thus $5\xi^5 + 5a\xi^3 + a^2\xi$.

35. The case $p^n = 3^n = 5m+3$.

The condition (2) of § 31 becomes since $m \equiv 21 \pmod{27}$,

$$c_6^{m+4} \cdot 20a^3\gamma^3 + c_9^{m+4}a^9 \equiv a^3\gamma^3 + a^9 = 0.$$

Hence $5\gamma = a^2$.

36. The case $p^n = 2^n = 5m + 3$, supposing $n > 3$. Thus $5m \equiv -3 \pmod{2^7}$ or $m \equiv 25 \pmod{128}$.

The powers $m + 2$ and $m + 4$ of $\xi^5 + a\xi^3 + \beta\xi^2 + \gamma\xi$ give

$$\gamma^2 + a^2\gamma + a\beta^2 = 0$$
$$a\gamma^4 + a^9 = 0.$$

Hence if $a = 0$, $\gamma = 0$; if $a \neq 0$, $\gamma = a^2$, $\beta = 0$.

But the power $m + 22$ of $\xi^5 + \beta\xi^2$ requires

$$c_{36}^{m+22} \cdot \beta^{36} \equiv \beta^{36} = 0.$$

The only possible form is again $5\xi^5 + 5a\xi^3 + a^2\xi$.

* *American Journal of Mathematics*, vol. 18, p. 213.

37. The case $p^n = 2^3$.

The third and fifth powers require respectively

$$\gamma^2 + \alpha^2\gamma + \alpha\beta^2 = 0$$

$$\gamma + \alpha\gamma^4 + \alpha^4\beta = 0\,,$$

of which the former is the square of the latter. Hence either $\alpha = \gamma = 0$ or $\beta = \alpha^3\gamma + \alpha^4\gamma^4$.

But $\xi^5 + \beta\xi^2$ vanishes for $\xi = \beta^{1/3}$, every mark in the $GF[2^3]$ being a cube by § 18.

By replacing ξ by $\alpha^{1/2}\xi$ and γ by $\alpha^2\gamma$, the quintic

$$\varphi(\xi) \equiv \xi^5 + \alpha\xi^3 + (\alpha^3\gamma + \alpha^4\gamma^4)\,\xi^2 + \gamma\xi$$

becomes

$$\alpha^{5/2}\{\xi^5 + \xi^3 + (\gamma + \gamma^4)\,\xi^2 + \gamma\xi\}.$$

Hence the quintic $\varphi(\xi)$ will vanish only for $\xi = 0$ if the resultant of

$$\xi^5 + \xi^3 + (\gamma + \gamma^4)\,\xi^2 + \gamma\xi \text{ and } \xi^7 = 1$$

is $\neq 0$. This resultant may be written as a cyclic determinant whose first row is

$$0,\ 1,\ 0,\ 1,\ \gamma + \gamma^4,\ \gamma,\ 0\,.$$

On expansion it becomes

$$\gamma^7 + \gamma^6 + \gamma^5 + \gamma^4 + \gamma^3 + \gamma^2 + \gamma = (\gamma^8 - \gamma)/(\gamma - 1)\,,$$

which is $\neq 0$ only when $\gamma = 1$.

The only suitable quintic on 8 letters is thus

$$\xi^5 + \alpha\xi^3 + \alpha^2\xi\,.$$

38. Summary of §§ 31–37. The only possible substitution quantic on $p^n = 5m + 3$ letters is reducible to the form

$$5\xi^5 + 5a\xi^3 + a^2\xi\,,\quad a \text{ arbitrary}\,,$$

except for $p^n = 13$ when we have the additional form

$$5\xi^5 + 5a\xi^3 + 2a^2\xi\,,$$

a being a quadratic non-residue of 13.

39. Theorem. *$5\xi^5 + 5a\xi^3 + a^2\xi$, where a is an arbitrary mark of the $GF[p^n]$, is suitable to represent a substitution on its p^n marks, if p is a prime number of the form $5m \pm 2$ and n is odd.*

For if not we must have for two different values of ξ, say η and φ, the following equation :

$$5\eta^5 + 5\alpha\eta^3 + \alpha^2\eta = 5\varphi^5 + 5\alpha\varphi^3 + \alpha^2\varphi$$

or

$$(\eta - \varphi)\{5(\eta^4 + \eta^3\varphi + \eta^2\varphi^2 + \eta\varphi^3 + \varphi^4) + 5\alpha(\eta^2 + \eta\varphi + \varphi^2) + \alpha^2\} = 0.$$

Hence since $\eta \neq \varphi$,

$$5\{\eta^4 + \varphi^4 + (\eta\varphi + \alpha)(\eta^2 + \eta\varphi + \varphi^2)\} + \alpha^2 = 0. \tag{1}$$

(a) Suppose $p > 2$.

Making the substitution

$$\eta = \lambda + \mu, \quad \varphi = \lambda - \mu$$

$$5\{5\lambda^4 + 10\lambda^2\mu^2 + \mu^4 + 3\alpha\lambda^2 + \alpha\mu^2\} + \alpha^2 = 0.$$

Multiply by 16 and substitute

$$20\lambda^2 = 4\rho - \alpha, \quad 4\mu^2 = 4\sigma - \alpha.$$

We thus reach the simple form

$$16(\rho^2 + 10\rho\sigma + 5\sigma^2) = 0,$$

or

$$(\rho + 5\sigma)^2 = 20\sigma^2 = 5(2\sigma)^2.$$

But* $+5$ is a quadratic residue of *no* odd number of the form $5m + 2$ or $5m + 3$. Hence 5 is a not-square in the $GF[p^n]$, n being odd and $p = 5m \pm 2$.

(b) Suppose $p = 2$.

Making in (1) the substitution

$$\eta + \varphi = \lambda, \quad \eta \cdot \varphi = \mu,$$

$$\lambda^4 + \alpha\lambda^2 + \alpha^2 = \mu(\lambda^2 + \mu + \alpha). \tag{2}$$

Put $\lambda^2 = \nu$ and multiply through by $\nu + \mu$:

$$\nu^3 + \alpha\nu^2 + \alpha^2\nu = \mu^3 + \alpha\mu^2 + \alpha^2\mu. \tag{3}$$

But, by § 18, ξ^3 is suitable to represent a substitution on 2^n letters, n odd, and hence is also

$$(\xi + \alpha)^3 + \alpha^3 = \xi^3 + \alpha\xi^2 + \alpha^2\xi.$$

Hence (3) has no solution in the $GF[2^n]$ except $\nu = \mu$, when by (2) we find $\nu = \mu = \alpha$.

* Gauss, *Disquisitiones Arithmetical*, Art. 121.

Hence if (1) is satisfied, we have

$$\eta + \varphi = \alpha^{1/2}, \quad \eta\varphi = \alpha .$$

But this set of values for η and φ is impossible since

$$\omega^2 + \alpha^{1/2}\omega + \alpha = 0$$

has no root in the $GF[2^n]$, n odd, if $\alpha \neq 0$, i. e. if $\eta \neq \varphi$. For writing $\omega = \alpha^{1/2}\theta$, it becomes

$$\theta^2 + \theta + 1 = 0 .$$

We thus need only prove that $\theta^3 - 1 = 0$ has no root other than $\theta = 1$ in the $GF[2^n]$, n odd. But if there exists a root $\neq 1$ of

$$\theta^{2^2-1} - 1 = 0$$

(and thus having the exponent 3) which is also a root of

$$\theta^{2^n-1} - 1 = 0 ,$$

then* must n be even.

A general theorem comprising the one here proven is given in § 54.

40. The case $p^n = 5m + 4$.

The power $m + 1$ of $\xi^5 + \alpha\xi^3 + \beta\xi^2 + \gamma\xi$ gives $\alpha = 0$.

The power $m + 2$ of $\xi^5 + \beta\xi^2 + \gamma\xi$ requires

$$c_2^{m+2} \cdot 2\beta\gamma = 0 .$$

Hence if $p \neq 2, \neq 3$, we have $\beta\gamma = 0$.

The power $m + 3$ requires, if $p^n > 9$,

$$c_3^{m+3}\gamma^3 + c_4^{m+3}\beta^4 = 0 .$$

Now $m + 3$ is divisible by p only if $p = 11$, when p^n is not of the form $5m + 4$. If $p = 2$ (and thus $n \geqq 6$, we have $m \equiv 12 \pmod{64}$. Hence for every $p^n > 9$,

$$5\gamma^3 = \beta^4 .$$

Thus for $p \neq 2, \neq 3$, $\beta = \gamma = 0$ and ξ^5 is the only suitable form.

41. The case $p^n = 3^n = 5m + 4$, $n > 2$.

The power $m + 4$ requires, since $m \equiv 1 \pmod{9}$,

$$c_5^{m+4} \cdot 10\beta^3\gamma^2 = \beta^3\gamma^2 = 0 .$$

Hence ξ^5 is the only suitable quintic.

* Moore, l. c. § 46.

42. The case $p^n = 3^2$.

The fourth, fifth, and seventh powers of $\xi^5 + \beta\xi^2 + \gamma\xi$ require respectively,

$$\gamma(1 + \gamma^2) + \beta^4 = 0$$

$$\beta^3(1 + \gamma^2) = 0$$

$$\beta(1 + \gamma^6) = 0 .$$

The solutions of these equations are

$$\beta = 0 , \ \gamma = 0 \quad \text{and} \quad \beta = 0 , \ \gamma^2 + 1 = 0 .$$

The suitable forms are thus

$$\xi^5 \text{ and } \xi^5 + 2^{1/2}\xi ,$$

since if the latter vanished for $\xi \neq 0$, $\xi^8 = 2$. Indeed $\xi^5 + 2^{1/2}\xi$ represents the literal substitution,

$$(0)(1, 1 + 2^{1/2})(-1, -1 - 2^{1/2})(2^{1/2}, -1 + 2^{1/2})(-2^{1/2}, 1 - 2^{1/2}) .$$

43. The case $p^n = 2^n = 5m + 4$.

The power $m + 11$ requires, since $m = 64l + 12$,

$$c_{17}^{m+11} \cdot 17\beta^{16}\gamma = \beta^{16}\gamma = 0 .$$

Hence $\beta = \gamma = 0$ and ξ^5 is the only suitable form.

44. Summary of §§ 40–43. ξ^5 is the only reduced substitution quintic on $p^n = 5m + 4$ letters, except for $p^n = 3^2$ when we have also $\xi^5 + 2^{1/2}\xi$.

45. $\xi^6 + \alpha\xi^4 + \beta\xi^3 + \gamma\xi^2 + \delta\xi$.

$p^n = 6m + 5$, since here p is prime to 6 and since $p^n \neq 6m + 1$.

The power $m + 1$ requires $\alpha = 0$.

The power $m + 2$ of $\xi^6 + \beta\xi^3 + \gamma\xi^2 + \delta\xi$ requires

$$2\beta\delta + \gamma^2 = 0 . \tag{1}$$

The power $m + 3$ requires, if $p^n > 11$,

$$6\gamma\delta^2 + m(2\beta^3\delta + 3\beta^2\gamma^2) = 0 . \tag{2}$$

The power $m + 4$ requires, if $p^n > 17$,

$$\delta^4 + \frac{m}{5}(30\beta^2\gamma\delta^2 + 20\beta\gamma^3\delta + \gamma^5) + \frac{m(m-1)}{5 \cdot 6}(6\beta^5\delta + 15\beta^4\gamma^2) = 0 . \tag{3}$$

Substituting γ^2 from (1) into (2) and (3),

$$6\gamma\delta^2 - 4m\beta^3\delta = 0 \tag{4}$$

$$\delta^4 - \frac{6m}{5}\beta^2\gamma\delta^2 - \frac{4m(m-1)}{5}\beta^5\delta = 0\,. \tag{5}$$

From (4) and (5)

$$\delta^4 - \frac{4m(2m-1)}{5}\beta^5\delta = 0\,. \tag{6}$$

Multiplying (1) by $m\beta^2$ and subtracting from (2),

$$6\gamma\delta^2 + 2m\beta^2\gamma^2 = 0\,.$$

If $p = 5$, $m \equiv 0 \pmod 5$, so that $\gamma\delta^2 = 0$ and then by (6) $\delta = 0$. If $p \neq 5$, suppose $\gamma \neq 0$. Then

$$m\beta^2\gamma = -3\delta^2\,.$$

Substituting this in (5),

$$23\delta^4 - 4m(m-1)\beta^5\delta = 0\,.$$

Combining with (6),

$$(41m - 18)\delta^4 = 0 \text{ or } 313\delta^4 = 0\,.$$

Since 313 is a prime not of the form $6m + 5$, $\delta = 0$. Hence must $\gamma = 0$, so that $\beta\delta = 0$ and by (6) $\delta = 0$. But the power $3m + 2$ of $\xi^6 + \beta\xi^3$ gives ξ^{18m+12} and no other term with exponent divisible by $6m + 4$. Hence there is no suitable sextic when $p^n > 17$. I have shown* that $p = 17, n = 1$ leads to no suitable septic; while $p = 11, n = 1$ leads to the following substitution quantics:

$\xi^6 \pm c^2\xi^3 + c\xi^2 \pm 5\xi$, c being a quadratic residue of 11.

$\xi^6 \pm 4c^2\xi^3 + c\xi^2 \pm 4\xi$, $c = 0$ or a quadratic non-residue of 11.

$\xi^6 \pm 2\xi$.

A preliminary study of septics, §§ 46–50.

$$\xi^7 + \alpha\xi^5 + \beta\xi^4 + \gamma\xi^3 + \delta\xi^2 + \varepsilon\xi\,.$$

46. The case $p^n = 7m + 6$.
The power $m + 1$ requires $\alpha = 0$.
The power $m + 2$ requires, if $p \neq 2$,

$$7\beta\varepsilon + 7\gamma\delta - \beta^3 = 0\,. \tag{1}$$

* *American Journal of Mathematics*, Vol. 18, pp. 216–217.

The power $m + 3$ requires, if $p > 5$ and $p^n \neq 13$,

$$7^2(\gamma\varepsilon^2 + \delta^2\varepsilon) - 7(6\beta^2\gamma\varepsilon + 3\beta^2\delta^2 + 6\beta\gamma^2\delta + \frac{1}{2}\gamma^4) + \frac{13}{2}\beta^4\gamma = 0. \qquad (2)$$

Rejecting the special values, 2, 5, 13, etc., we may prove that if any *one* of the four coefficients $\beta, \gamma, \delta, \varepsilon$ be zero, then all are zero. To handle (1), (2), and the very lengthy conditions given by the powers $m + 4$ and $m + 5$; when $\beta, \gamma, \delta, \varepsilon$ are all $\neq 0$, is perhaps impracticable.

Suppose, for example, $\gamma = 0$. Then (1) and (2) become

$$\beta^3 = 7\beta\varepsilon\,;\quad 7\delta^2\varepsilon = 3\beta^2\delta^2.$$

Thus $\delta = 0$; for if not

$$7\varepsilon = 3\beta^2 \text{ and thus } \beta^3 = 3\beta^3.$$

The power $m + 5$ of $\xi^7 + \beta\xi^4 + \varepsilon\xi$ requires

$$7^5\varepsilon^5 - 7^4 \cdot 15\beta^2\varepsilon^4 + 7^3 \cdot 65\beta^4\varepsilon^3 - 7^2 \cdot 130\beta^6\varepsilon^2 + \frac{65 \cdot 27}{2}\beta^8\varepsilon - \frac{13 \cdot 51}{14}\beta^{10} = 0.$$

If $\beta \neq 0$, $\beta^2 = 7\varepsilon$ and the last equation becomes $-\beta^{10} = 0$. Thus if $\gamma = 0$, then $\beta = \delta = \varepsilon = 0$, certain values of p^n being excepted.

47. The case $p^n = 7m + 5$.

The power $m + 1$ requires $\beta = 0$. If either α, γ, or ε be zero, we can prove that all are zero. If $\delta = 0$, the conditions given by the powers $m + 2$ and $m + 4$ (of 5 and 19 terms respectively) are satisfied by

$$7\gamma = 2\alpha^2,\quad 7^2\varepsilon = \alpha^3.$$

48. The case $p^n = 7m + 4$.

The power $m + 1$ requires, if $p \neq 3$,

$$7\gamma = 2\alpha^2.$$

We may prove that if $\alpha = 0$, then $\beta = \gamma = \delta = \varepsilon = 0$; that if $\beta = 0$ then $\delta = 0$ and $7^2\varepsilon = \alpha^3$.

49. The case $p^n = 7m + 3$.

The power $m + 1$ requires, if $p \neq 2$, $7\delta = 3\alpha\beta$.

We may prove that if $\alpha = 0$, then $\beta = \gamma = \delta = \varepsilon = 0$; if $\beta = 0$ then $\delta = 0$ and the conditions given by the powers $m + 2$ and $m + 4$ (containing seven and twenty-one terms respectively) are seen to be satisfied by

$$7\gamma = 2\alpha^2,\quad 7^2\varepsilon = \alpha^3.$$

50. The case $p^n = 7m + 2$.

The conditions are quite unwieldly even when $\alpha = 0$. If $\beta = 0$, then $\delta = 0$, $7\delta = 2\alpha^2$, $7^2\varepsilon = \alpha^3$.

Quantics with an infinite range of suitability, §§ 51–56.

51. We have found that the quintic

$$5\xi^5 + 5\alpha\xi^3 + \alpha^2\xi\,,$$

α being an arbitrary mark of the $GF[p^n]$, is suitable to represent a substitution on its p^n marks, if and only if p^n be of the form $5m \pm 2$. Also in our preliminary survey of septics, the quantic

$$7^2\xi^7 + 7^2\alpha\xi^5 + 2\,.\,7\alpha^2\xi^3 + \alpha^3\xi\,,$$

α being an arbitrary mark of the $GF[p^n]$, stood out in a prominent way as probably suitable on its p^n marks if and only if p^n be of the form $7m \pm 2$ or $7m \pm 3$. Note further that there is no suitable cubic other than ξ^3. Thus is suggested the possible existence of a quantic of odd prime degree k which is suitable to represent a substitution on the marks of every $GF[p^n]$, except when p^n is of the form $km \pm 1$.

52. Suppose the reduced quantic belonging to the $GF[p^n]$,

$$\xi^k + a_2\xi^{k-2} + a_3\xi^{k-3} + a_4\xi^{k-4} + \ldots + a_{k-1}\xi\,, \tag{1}$$

whose degree k is an odd prime number $\neq p$, is suitable to represent a substitution on the p^n marks of the field for every p^n of the form $km + 2$, $km + 3$, $km + 4$, $\ldots$, or, $km + (k - 3)$. We do not at first assume it suitable on $p^n = km + (k - 2)$ letters, in which case the power $m + 1$ requires

$$(m + 1)\,a_3 = a_3 = 0, \text{ if } p \neq 2.$$

For $p^n = km + (k - 3)$, the power $m + 1$ requires

$$(m + 1)\,a_4 + \frac{(m + 1)m}{2}\,a_2^2 = 0\,,$$

or, if $p \neq 3$,

$$ka_4 = \frac{k - 3}{2}\,a_2^2\,.$$

For $p^n = km + (k - 4)$, the power $m + 1$ requires if $p \neq 2$,

$$ka_5 = (k - 4)\,a_2a_3\,.$$

For $p^n = km + (k - 5)$, the power $(m + 1)$ requires, if $p \neq 5$,

$$k^2a_6 - \frac{k\,(k - 5)}{2}\,(a_3^2 + 2a_2a_4) + \frac{(k - 5)\,(2k - 5)}{2\,.\,3}\,a_2^3 = 0\,,$$

or

$$k^2 a_6 = \frac{(k-4)(k-5)}{2 \cdot 3} a_2^3 + \frac{k(k-5)}{2} a_3^2 .$$

For $p^n = km + (k-6)$, the power $m+1$ requires, if $p \neq 2, \neq 3$,

$$k^2 a_7 - k(k-6)(a_2 a_5 + a_3 a_4) + \frac{(k-6)(2k-6)}{2} a_2^2 a_3 = 0 ,$$

or

$$k^2 a_7 = \frac{(k-5)(k-6)}{2} a_2^2 a_3 .$$

Similarly, for $p^n = km + (k-7)$, the power $m+1$ requires, if $p \neq 7$,

$$k^3 a_8 = \frac{(k-5)(k-6)(k-7)}{2 \cdot 3 \cdot 4} a_2^4 + \frac{k(k-6)(k-7)}{2} a_2 a_3^2 ;$$

for $p^n = km + (k-8)$, p $\neq 2$, the power $m+1$ requires

$$k^3 a_9 = \frac{(k-6)(k-7)(k-8)}{2 \cdot 3} a_2^3 a_3 + \frac{k(k-7)(k-8)}{2 \cdot 3} a_3^3 ;$$

for $p^n = km + (k-9)$, $p \neq 3$, the power $m+1$ requires

$$k^4 a_{10} = \frac{(k-6)(k-7)(k-8)(k-9)}{2 \cdot 3 \cdot 4 \cdot 5} a_2^5 + \frac{k(k-7)(k-8)(k-9)}{4} a_2^2 a_3^3 .$$

It would be impracticable to attempt to calculate the general coefficient in this way. It is to be noted that if $p > k$ every coefficient is expressed uniquely in terms of a_2 and a_3.

53. The sum s_k of the kth powers of the roots of the cubic

$$\eta^3 - \xi\eta^2 - \frac{a_2}{k}\eta - \frac{a_3}{k} = 0 \tag{2}$$

is given by Waring's formula thus :

$$s_k = \sum_{\lambda} \frac{\pi(\lambda_1 + \lambda_2 + \lambda_3 - 1)}{\pi(\lambda_1)\,\pi(\lambda_2)\,\pi(\lambda_3) \cdot k^{\lambda_2+\lambda_3-1}} \cdot a_2^{\lambda_2} a_3^{\lambda_3} \xi^{\lambda_1} \tag{3}$$

where $\pi(t) = t!$ with the convention that $\pi(0) = 1$, and where the summation extends over $\lambda_1, \lambda_2, \lambda_3$ such that

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 = k .$$

Arranging according to descending powers of ξ, we have

$$s_k = \xi^k + a_2\xi^{k-2} + a_3\xi^{k-3} + \frac{k-3}{2k}a_2^2\xi^{k-4} + \frac{k-4}{k}a_2a_3\xi^{k-5}$$
$$+ \left\{\frac{(k-4)(k-5)}{6k^2}a_2^3 + \frac{k-5}{2k}a_3^2\right\}\xi^{k-6} + \frac{(k-5)(k-6)}{2k^2}a_2^2a_3\xi^{k-7}$$
$$+ \left\{\frac{(k-5)(k-6)(k-7)}{24k^3}a_2^4 + \frac{(k-6)(k-7)}{2k^2}a_2a_3^2\right\}\xi^{k-8}$$
$$+ \left\{\frac{(k-6)(k-7)(k-8)}{6k^3}a_2^3a_3 + \frac{(k-7)(k-8)}{6k^2}a_3^3\right\}\xi^{k-9}$$
$$+ \left\{\frac{(k-6)(k-7)(k-8)(k-9)}{5!\,k^4}a_2^5 + \frac{(k-7)(k-8)(k-9)}{4k^3}a_2^2a_3^2\right\}\xi^{k-10} + \ldots. \quad (4)$$

Thus the first ten coefficients in s_k are exactly the corresponding coefficients of the quantic (1) as calculated in § 52. A complete identification of s_k with (1) will be carried out for the most interest case, viz, when $a_3 = 0$, which happens when the range of suitability of (1) excludes only the combinations $p^n = km \pm 1$. For then by § 54 the quantic $s_k(\xi)$ will satisfy the conditions derived by the method of § 52 which have an unique solution in terms of a_2.

For $a_3 = 0$, (3) reduces to

$$s_k = \sum_{l=0}^{(k-1)/2}{}' \frac{\pi(k-l-1)}{\pi(l)\,\pi(k-2l)}\,a_2^l/_{k^{l-1}}\cdot\xi^{k-2l}.$$

Thus

$$\eta_1^k + \eta_2^k = \xi^k + k\cdot\sum_{l=1}^{(k-1)/2}{}' \frac{(k-l-1)(k-l-2)\ldots(k-2l+1)}{2\cdot 3\ldots l}\left[\frac{a_2}{k}\right]^l\xi^{k-2l}, \quad (5)$$

where η_1 and η_2 are the roots of the quadratic

$$\eta^2 - \xi\eta - \frac{a^2}{k} = 0. \quad (6)$$

54. Theorem. *The quantic*

$$\theta_k(\xi, a) \equiv \xi^k + k\sum_{l=1}^{(k-1)/2}{}' \frac{(k-l-1)\ldots(k-2l+1)}{2\cdot 3\ldots l}\,a^l\xi^{k-2l},$$

where k is any odd integer not divisible by p, and a any mark except† zero of the $GF[p^n]$, is suitable to represent a substitution on its p^n marks, if and only if p^{2n-1} be relatively prime to k.*

* k is not necessarily prime. The proof in § 52 that $\theta_k(\xi, a)$ is the *only* quantic with the range of suitability $p^n = km + 2, + 3, \ldots + (k-2)$ requires that k be a prime number.

† See § 18.

We are to prove that under the named restrictions

$$\theta_k(\xi, \alpha) = \beta \tag{7}$$

has a solution ξ in the $GF[p^n]$, β being an arbitrary mark of that field.

Now by the transformation

$$\xi = \eta - \frac{\alpha}{\eta} \tag{6'}$$

the quantic is given the form

$$\eta^k - \left[\frac{\alpha}{\eta}\right]^k. \tag{5'}$$

Thus equation (7) becomes

$$\eta^{2k} - \beta\eta^k - \alpha^k = 0\,. \tag{7'}$$

Substituting $Y = \eta^k$, this becomes

$$Y^2 - \beta Y + (-\alpha)^k = 0\,,$$

which *belongs* to the $GF[p^n]$ and is for *every* β resolvable in the $GF[p^{2n}]$ but not in the $GF[p^n]$. Call its roots Y and $\overline{Y}$.

Now the equation

$$\eta^k = Y$$

is solvable in the $GF[p^{2n}]$, Y being an arbitrary mark of that field, if and only if $p^{2n} - 1$ be relatively prime to k.

Then if η be a mark of the $GF[p^{2n}]$ satisfying (7'), we must prove that

$$\xi = \eta - \frac{\alpha}{\eta}$$

falls into the lower field $GF[p^n]$. Since Y and $\overline{Y}$ are conjugate marks with respect to the $GF[p^n]$ whose product is $(-\alpha)^k$, we have

$$\eta\bar{\eta} = -\alpha\,.$$

Hence

$$\xi = \eta - \alpha/\eta = \eta + \bar{\eta} = \bar{\xi}$$

so that indeed* ξ belongs to the $GF[p^n]$.

55. The *algebraic* roots of (7) are

$$\rho\varepsilon^m + \sigma\varepsilon^{k-m} \qquad (m = 0, 1, \ldots, k-1)$$

where

$$\rho, \sigma = \sqrt[k]{\beta/2 \pm \sqrt{\beta^2/4 + \alpha^k}}$$

* Moore, l. c. § 51.

and ε is a primitive kth root of unity. This is a straight generalization of Cardan's formula for the roots of the cubic and also of Vallès' solution of the quintic*

$$x^5 + \alpha x^3 + \frac{\alpha^2}{5} x - \beta = 0 .$$

It is evident that the algebraic solution of (7) for α and β arbitrary is equivalent to the extraction of the kth root of an arbitrary complex quantity and hence equivalent to the partitioning of an arbitrary angle into k equal parts.

56. The study of the quantic $\varphi_k(\xi, a_2, a_3)$ derived as in § 52, or conjecturally (when $a_3 \neq 0$) as in § 53, is made here only for the case $a_3 = 0$. It is to be expected that, for $a_3 \neq 0$, it is a substitution quantic at least for certain special values of k, p, n, a_2 and a_3. Thus if $k = 5$, $p = 7$, we find

$$\xi^5 + a_2\xi^3 + a_3\xi^2 + 3a_2^2\xi$$

which by § 30 includes the three types of quintics suitable on 7 letters, as well as the one suitable on 7^n letters, n being odd.

Section III.—*Degree a Power of p.*

Quantics with all exponents powers of p, §§ 57–59.

57. Theorem.† The reduced quantic

$$\chi(X) = \sum_{i=1}^{m} A_i X^{p^{n(m-i)}},$$

belonging to the $GF[p^{nm}]$, will represent a substitution on its p^{nm} marks if and only if

$$\chi(X) = 0 \tag{1}$$

has no root in the $GF[p^{nm}]$ other than $X = 0$.

For it will be a substitution quantic if and only if it be impossible to find two different marks X_1 and X_2 of the $GF[p^{nm}]$ such that

$$\chi(X_1) = \chi(X_2)$$

or

$$\chi(X_1 - X_2) = 0 .$$

Corollary. $X^{p^{nr}} - AX^{p^{ns}}$ represents a substitution on p^{nm} letters if and only if $A = 0$ or A is a not $(p^{nr} - p^{ns})$ power in the $GF[p^{nm}]$.

---

* M. F. Vallès, *Formes imaginaires en Algèbre*, Vol. I, pp. 90–92, 1869.

† I reached this result independently. Cf. Mathieu, l. c. Vol. 6, 1861, p. 275; also Betti, l. c. Vol. 3, p. 74, 1852. For the connection with linear substitutions see Part II, Section III.

58. Since every mark except $X = 0$ of the $GF[p^{nm}]$ satisfies the equation

$$X^{p^{nm}-1} - 1 = 0\,, \tag{2}$$

it follows from § 57 that $\chi(X)$ will represent a substitution on p^{nm} letters if and only if the resultant of (2) and (1) is different from zero. This resultant is

$$\begin{vmatrix} A_1 & , & A_2 & , & \ldots, & A_m \\ A_2^{p^n} & , & A_3^{p^n} & , & \ldots, & A_1^{p^n} \\ A_3^{p^{2n}} & , & A_4^{p^{2n}} & , & \ldots, & A_2^{p^{2n}} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ A_m^{p^{n(m-1)}} & , & A_1^{p^{n(m-1)}} & , & \ldots, & A_{(m-1)}^{p^{n(m-1)}} \end{vmatrix}. \tag{3}$$

The proof is analogous to Sylvester's dialytic method. I set up m equations linear and homogeneous in the m quantities

$$X^{p^{n(m-i)}} - 1\,, \qquad (i = 1, 2, \ldots, m)$$

such that the system of m equations is equivalent to the system (1) and (2).

Thus, raising $\chi(X)$ to the p^{nk} power,

$$\sum_{i=1}^{m}{}' A_i^{p^{nk}} X^{p^{n(n+k-i)}} = 0\,.$$

Applying (2) multiplied by X to the first k terms,

$$\sum_{i=1}^{k}{}' A_i^{p^{nk}} X^{p^{n(k-i)}} + \sum_{i=k+1}^{m}{}' A_2^{p^{nk}} X^{p^{n(m+k-i)}} = 0\,.$$

Introducing in each a new summation index,

$$\sum_{j=m-k+1}^{m}{}' A_{j+k-m}^{p^{nk}} X^{p^{n(m-j)}} + \sum_{j=1}^{m-k}{}' A_{j+k}^{p^{nk}} X^{p^{n(m-j)}} = 0\,.$$

Combining and replacing the index j by i,

$$\sum_{i=1}^{m}{}' A_{i+k}^{p^{nk}} X^{p^{n(m-i)}} = 0\,, \tag{4}$$

where, if $i + k > m$, we are to understand

$$A_{i+k} = A_{i+k-m}\,.$$

Dividing out X from (4) we obtain for $k = 0, 1, 2, \ldots, m-1$ a system of m equations equivalent to the system (1) and (2), since from the former we can pass back to the latter.

59. Owing to the objection that may be made against the usual proof of Sylvester's dialytic method of elimination, the following proof that (3) is the resultant of (1) and (2) is given.

Lemma.* The necessary and sufficient condition that m marks $\Omega_0, \Omega_1, \ldots, \Omega_{m-1}$ of the $GF[p^{nm}]$ shall be linearly independent with respect to the $GF[p^n]$ is that the determinant

$$\begin{vmatrix} \Omega_0 & , & \Omega_1 & , & \ldots, & \Omega_{m-1} \\ \Omega_0^{p^n} & , & \Omega_1^{p^n} & , & \ldots, & \Omega_{m-1}^{p^n} \\ \Omega_0^{p^{2n}} & , & \Omega_1^{p^{2n}} & , & \ldots, & \Omega_{m-1}^{p^{2n}} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \Omega_0^{p^{n(m-1)}} & , & \Omega_1^{p^{n(m-1)}} & , & \ldots, & \Omega_{m-1}^{p^{n(m-1)}} \end{vmatrix} = \Omega_j^{p^{ni}} |, \quad (j^i = 0, 1, \ldots, m-1) \tag{5}$$

shall $\neq 0$.

It is sufficient; for if $\Omega_0, \Omega_1, \ldots, \Omega_{m-1}$ be linearly dependent in the $GF[p^n]$, i. e. if a relation

$$\sum_{i=0}^{m-1} \gamma_i \Omega_i = 0 \tag{6}$$

holds where $\gamma_0, \gamma_1, \ldots, \gamma_{m-1}$ are marks of the $GF[p^n]$ not all zero, then will the determinant (5) vanish.

It is necessary; for if (5) be zero, write

$$\Omega_i = \sum_{j=0}^{m-1} \mu_{ij} R^j \qquad (i = 0, 1, \ldots, m-1)$$

where R is a primitive root of the $GF[p^{nm}]$ and the μ_{ij}'s are marks of the $GF[p^n]$. Then

$$| \Omega_j^{p^{ni}} | = | \mu_{ij} | \cdot | (R^j)^{p^{ni}} |, \quad (i, j = 0, 1, \ldots, m-1)$$

* A more general theorem is given by E. H. Moore, *A two-fold generalization of Fermat's theorem*, *Bulletin of the American Mathematical Society*, second series, Vol. 2, April, 1896.

where, writing in full the determinant in R, we have*

$$\begin{vmatrix} 1 & , 1 & , \ldots, & 1 \\ R & , R^{p^n} & , \ldots, & R^{p^{n(m-1)}} \\ R^2 & , R^{2p^n} & , \ldots, & R^{2p^{n(m-1)}} \\ \cdot & \cdot & \cdot & \cdot \\ R^{m-1}, & R^{(m-1)p^n}, & \ldots, & R^{(m-1)p^{n(m-1)}} \end{vmatrix} = \Pi (R^{p^{ns}} - R^{p^{nt}}) \qquad \begin{matrix} s, t = 0, 1, \ldots, m-1 \\ s > t \end{matrix} \quad (7)$$

which $\neq 0$, R being a primitive root in the $GF[p^{nm}]$. Hence $|\mu_{ij}| = 0$, so that a linear relation (6) exists, in which not every γ_i is zero, or $\Omega_0, \Omega_1, \ldots, \Omega_{m-1}$ are linearly dependent in the $GF[p^n]$.

The condition on $A_1, A_2, \ldots, A_m$ that

$$X' = \sum_{i=1}^{m} A_i X^{p^{n(m-i)}} \qquad (8)$$

shall represent a substitution on p^{nm} letters is the same as the condition under which $X_1' X_2', \ldots, X_m'$ shall be linearly independent with respect to the $GF[p^n]$, when it is given that $X_1, X_2, \ldots, X_m$ are similarly independent. By our lemma, the latter condition is

$$|X_j'^{p^{ni}}| \neq 0 . \qquad (i, j = 0, 1, \ldots, m-1)$$

Applying (8) this determinant becomes

$$\begin{vmatrix} A_1 X_1^{p^{n(m-1)}} + A_2 X_1^{p^{n(m-2)}} + \ldots + A_m X_1 & , \ldots A_1 X_m^{p^{n(m-1)}} + \ldots + A_m X_m \\ A_1^{p^n} X_1 + A_2^{p^n} X_1^{p^{n(m-1)}} + \ldots + A_m^{p^n} X_1^{p^n} & , \ldots A_1^{p^n} X_m + \ldots + A_m^{p^n} X_m^{p^n} \\ A_1^{p^{2n}} X_1^{p^n} + A_2^{p^{2n}} X_1 + \ldots + A_m^{p^{2n}} X_1^{p^{2n}}, & \ldots A_1^{p^{2n}} X_m^{p^n} + \ldots + A_m^{p^{2n}} X_m^{p^{2n}} \\ \cdot & \cdot \end{vmatrix}$$

which equals the product of determinant (3) of § 58 by

$$\begin{vmatrix} X_1^{p^{n(m-1)}}, & X_2^{p^{n(m-1)}}, & \ldots, & X_m^{p^{n(m-1)}} \\ X_1^{p^{n(m-2)}}, & X_2^{p^{n(m-2)}}, & \ldots, & X_m^{p^{n(m-2)}} \\ \cdot & \cdot & \cdot & \cdot \\ X_1 & , X_2 & , \ldots, & X_m \end{vmatrix} .$$

* Baltzer, *Determinanten*, p. 85.

But by (5) this $\neq 0$, $X_1, \ldots, X_m$ being supposed linearly independent in the $GF[p^n]$.

General theorems on $SQ[p^r; p^n]$, §§ 60–68.

60. In studying the quantic belonging to the $GF[p^n]$,

$$\xi^{p^r} + a_k\xi^{p^r-k} + a_{k+1}\xi^{p^r-k-1} + \ldots + a_{p^r-1}\xi,$$

in which $a_k \neq 0$, and $k < p^r - 1$ it is found desirable to compute the power

$$p^{n-r} + k(p^{n-2r} + p^{n-3r} + \ldots + p^{r+t}) + h,$$

where t is the least positive residue of n modulo r and $h < p^{r+t}$.

Let the general term of the expansion be

$$(\xi^{p^r})^{a_0} \cdot (a_k\xi^{p^r-k})^{a_k} \cdot (a_{k+1}\xi^{p^r-k-1})^{a_{k+1}} \ldots (a_{p^r-1}\xi)^{a_{p^r-1}},$$

where we thus have

$$a^0 + a_k + a_{k+1} + \ldots + a_{p^r-1} = p^{n-r} + kp^{n-2r} + \ldots + h, \qquad (1)$$

$$s \equiv p^r a_0 + (p^r - k)\, a_k + (p^r - k - 1)\, a_{k+1} + \ldots + a_{p^r-1} = p^n - 1. \qquad (2)$$

I shall use the abbreviations

$$s_1 \equiv p^r a_0 + (p^r - k)\, a_k + a_{k+1} + a_{k+2} + \ldots + a_{p^r-1};$$

$$s_2 \equiv p^r a_0 + (p^r - k)\, a_k + (p^r - k - 1)(a_{k+1} + a_{k+2} + \ldots + a_{p^r-1}).$$

61. By equation (2)

$$a_0 \leqq (p^n - 1)/p^r < p^{n-r}.$$

Hence by an application of § 14 to (1),

$$a_0 \leqq kp^{n-2r} + k \cdot p^{n-3r} + \ldots + k \cdot p^{r+t} + h.$$

Suppose at first

$$a_0 = k \cdot p^{n-2r} + k \cdot p^{n-3r} + \ldots + h - x,$$

where

$$0 \leqq x \leqq kp^{n-3r} + kp^{n-4r} + \ldots + h.$$

Then by (1)

$$a_k + a_{k+1} + \ldots + a_{p^r-1} = p^{n-r} + x.$$

If $a_k = p^{n-r} + y$, where $0 \leqq y \leqq x$, we readily find

$$s_1 = p^n + kp^{n-2r} + kp^{n-3r} + \ldots + hp^r - (p^r - 1)\, x + (p^r - k - 1)\, y.$$

$$\geqq p^n + kp^{n-2r} + \ldots + hp^r - p^r x > p^n - 1.$$

Hence $s \geqq s_1 > p^n - 1$, contrary to (2).

If $a_k = y$, then

$$s_2 = (p^r - 1)\,p^{n-r} + k\,.\,p^{n-2r} + kp^{n-3r} + \ldots + hp^r - (k+1)\,x + y\,.$$

Hence $s \equiv\!\!\!\!< s_2 < p^n - 1$.

Applying § 14, we conclude that $a_0 < kp^{n-2r}$ and thus

$$a_0 \equiv\!\!\!\!< (k-1)\,p^{n-2r} + kp^{n-3r} + \ldots + k\,.\,p^{r+t} + h\,.$$

62. We may prove by induction the theorem

$$a_0 \equiv\!\!\!\!< (k-1)\,(p^{n-2r} + p^{n-3r} + \ldots + p^{r+t}) + h\,.$$

Thus, to make the general step, suppose

$$a_0 = (k-1)\,(p^{n-2r} + p^{n-3r} + \ldots + p^{n-mr}) + k\,(p^{n-(m+1)r} + p^{n-(m+2)r} + \ldots + p^{r+t}) + h - x'\,,$$

where

$$0 \equiv\!\!\!\!< x' \equiv\!\!\!\!< k\,(p^{n-(m+2)r} + p^{n-(m+3)r} + \ldots + p^{r+t}) + h\,.$$

Then

$$a_k + a_{k+1} + \ldots + a_{p^r-1} = p^{n-r} + p^{n-2r} + \ldots + p^{n-mr} + x'\,.$$

If $a_k = p^{n-r} + p^{n-2r} + \ldots + p^{n-mr} + y'$, $0 \equiv\!\!\!\!< y' \equiv\!\!\!\!< x'$, then

$$s_1 = p^n + k\,(p^{n-(m+1)r} + \ldots + p^{2r+t}) + hp^r - (p^r - 1)\,x' + (p^r - k - 1)\,y'\,.$$

Hence $s \equiv\!\!\!\!> s_1 > p^n - 1$.

If $a_k = p^{n-r} + p^{n-2r} + \ldots + p^{n-(m-1)r} + y'$,

$$s_2 = p^n - p^{n-mr} + k\,(p^{n-(m+1)r} + \ldots + p^{2r+t}) + hp^r - (k+1)\,x' + y'\,.$$

Hence $s \equiv\!\!\!\!< s_2 < p^n - 1$.

If a_k have a value less than that last supposed, much more will s be $< p^n - 1$. Hence

$$a_0 < (k-1)\,(p^{n-2r} + p^{n-3r} + \ldots + p^{n-mr}) + kp^{n-(m+1)r}\,.$$

Hence finally,

$$a_0 \equiv\!\!\!\!< (k-1)\,(p^{n-2r} + \ldots + p^{n-(m+1)r}) + k\,(p^{n-(m+2)r} + \ldots + p^{r+t}) + h\,.$$

63. Let g denote a positive integer and write

$$a_0 = (k-1)\,(p^{n-2r} + p^{n-3r} + \ldots + p^{r+t}) + h - g\,. \qquad (3)$$

Here g is not a multiple of p, since then would also $a_k + a_{k+1} + \ldots + a_{p^r-1}$ and by § 14 s would likewise be a multiple of p.

From (1), (2) and (3) we readily find

$$a_k + a_{k+1} + \ldots + a_{p^r-1} = p^{n-r} + p^{n-2r} + \ldots + p^{r+t} + g \tag{4}$$

$$(p^r - k)\,a_k + (p^r - k - 1)\,a_{k+1} + \ldots + a_{p^r-1} = p^n - 1 - p^r a_0$$

$$= (p^r - k)(p^{n-r} + p^{n-2r} + \ldots + p^{r+t}) + p^r(kp^t + g - h) - 1\,. \tag{5}$$

Multiplying (4) by $p^r - k$ and subtracting (5),

$$a_{k+1} + 2a_{k+2} + 3a_{k+3} + \ldots (p^r - k - 1)\,a_{p^r-1} = p^r(h - kp^t) - kg + 1\,. \tag{6}$$

Thus

$$g \leqq \{p^r(h - kp^t) + 1\}/k$$

$$h > kp^t, \text{ unless } h = k = 1,\ t = 0\,. \tag{7}$$

The calculation of the condition given by the power

$$p^{n-r} - k(p^{n-2r} + p^{n-3r} + \ldots + p^{r+t}) + h$$

consists in taking for g in turn each of the values*

$$1, 2, 3, \ldots E\left\{\frac{p^r(h - kp^t) + 1}{k}\right\}$$

and determining by (6) every possible set of values for $a_{k+1}, a_{k+2}, \ldots a_{p^r-1}$ which form a partition of

$$p^{n-r} + p^{n-2r} + \ldots + p^{r+t} + g$$

of the kind required by § 14. Then (4) gives the a_k and finally (3) the a_0 corresponding to each set.

64. The value $g = 1$ may be discarded if

$$kp^t < h \leqq (k+1)p^t,$$

provided $k > 1$ when the equality sign holds.

For by (5),

$$a_k < p^{n-r} + p^{n-2r} + \ldots + p^{r+t};$$

and hence by (4),

$$a_k \leqq p^{n-r} + p^{n-2r} + \ldots + p^{2r+t} + 1\,.$$

Then

$$s_2 \leqq (p^r - 1)(p^{n-r} + p^{n-2r} + \ldots + p^{2r+t}) + hp^r - k + p^{r+t}(p^r - k - 1)\,.$$

Hence

$$s \leqq s_2 \leqq p^n + hp^r - (k+1)p^{r+t} - k < p^{n-1}$$

if

$$h < (k+1)p^t \text{ or } h = (k+1)p^t, k > 1\,.$$

* $E(x)$ denotes the greatest integer in x.

65. Theorem. *If $t = 0$, i. e. n be a multiple of r, the coefficient $a_1 = 0$.*

For $p^r = 2$, $\xi^2 + a_1\xi$ is suitable on 2^n letters (by § 57) if and only if it vanishes only when $\xi = 0$ i. e. if $a_1 = 0$.

For $p^r > 2$, consider the power

$$p^{n-r} + p^{n-2r} + \ldots + p^r + 1 .$$

Making $h = k = 1$, $t = 0$, we have $g = 1$ and hence

$$a_0 = 0,\ a_1 = p^{n-r} + \ldots + p^r + 1,\ a_2 = a_3 = \ldots = a_{p^r-1} = 0 .$$

The condition is thus

$$a_1^{p^{n-r}+\ldots+p^r+1} = 0 .$$

66. Theorem. *If the quantic belonging to the GF $[p^n]$, $p > 2$,*

$$\xi^{p^r} + a_{\frac{p^r+1}{2}}\xi^{(p^r-1)/2} + a_{(p^r+3)/2}\xi^{(p^r-3)/2} + \ldots + a_{p^r-1}\xi$$

be suitable on p^n letters, then $a_{(p^r+1)/2} = 0$.

Consider the power

$$p^{n-r} + \frac{p^r+1}{2}(p^{n-2r} + p^{n-3r} + \ldots + p^{r+t} + p^t) + 1 .$$

Thus

$$k = (p^r + 1)/2,\ h = \frac{p^r+1}{2} \cdot p^t + 1,\ g = 2 .$$

Hence by (6) and (4)

$$a_{k+1} = a_{k+2} = \ldots = a_{p^r-1} = 0,\ a_k = p^{n-r} + p^{n-2r} + \ldots + p^{r+t} + 2 .$$

The condition is thus $a_k^{a_k} = 0$.

67. Less frequently will be studied the power

$$q \cdot p^{n-r} + k(p^{n-2r} + p^{n-3r} + \ldots + p^{r+t}) + h ,$$

where q and k are $< p^r$ and $h < p^{r+t}$.

Similarly as in §§ 61 and 62 we may prove that

$$a_0 < (q-1)p^{n-r} + (k-1)(p^{n-2r} + \ldots + p^{r+t}) + h .$$

Taking $s = q(p^n - 1)$, we find as in § 63,

$$a_0 = (q-1)p^{n-r} + (k-1)(p^{n-2r} + \ldots + p^{r+t}) + h - g$$

$$a_{k+2} + 2a_{k+2} + 3a_{k+3} + \ldots + (p^r - k - 1)a_{p^r-1} = p^r(h - kp^t) - kg + q ,$$

where $g > 0$, $g \not\equiv 0 \pmod{p}$.

The parts of the condition given by

$$s = q_1 (p^n - 1), \quad q_1 < q$$

can not be satisfactorily obtained by a similar analysis. See the direct method used in § 73 (f).

68. Exactly as in §§ 61–63, we may prove that for the

$$p^{n-r} + k (p^{n-2r} + p^{n-3r} + \ldots + p^{2r+t}) + (k+1) p^{r+t} + h$$

power of the quantic (in which the term $a_{k+1}\xi^{p^r-k-1}$ is absent)

$$\xi^{p^r} + a_k \xi^{p^r-k} + a_{k+2}\xi^{p^r-k-2} + \ldots + a_{p^r-1}\xi ,$$

$$a_0 = (k-1)(p^{n-2r} + \ldots + p^{2r+t}) + kp^{r+t} + h - g , \; g \equiv\!\!\!> 1 ;$$

$$a_k + a_{k+2} + a_{k+3} + \ldots + a_{p^r-1} = p^{n-r} + p^{n-2r} + \ldots + p^{r+t} + g ;$$

$$2a_{k+2} + 3a_{k+3} + \ldots + (p^r - k - 1) a_{p^r-1} = p^{2r+t} + hp^r - kp^{r+t} - kg + 1 .$$

Determination of all reduced SQ $[p^r ; p^n]$ *for* $p^r \equiv\!\!\!< 7$ *and partially for* $p^r = 11$, §§ 69–74.

69. $p^r = 2$.

By § 65 we need only consider ξ^2, which is suitable on 2^n letters by § 18.

70. $p^r = 3$.

By § 65 the form is $\xi^3 + a_2\xi$, which is suitable on 3^n letters by § 57, corollary, if and only if $a_2 = 0$, or $-a_2$ is a not-square in the $GF'[3^n]$.

71. $p^r = 2^2$. $\xi^4 + a_1\xi^3 + a_2\xi^2 + a_3\xi$ on 2^n letters.

If n be even, $a_1 = 0$ by § 65.

If n be odd, then also $a_1 = 0$. For if not we may remove the term ξ^2 by a linear transformation. Consider then the power $2^{n-2} + 2^{n-4} + \ldots + 2^3 + 3$ of

$$\xi^4 + a_1\xi^3 + a_3\xi .$$

Since $a_0 \equiv\!\!\!> 0$, it follows from (3) of § 63 that $g \equiv\!\!\!< 3$; also that $g \neq 2$. By § 64, $g > 1$. The remaining value $g = 3$ gives in equation (6) of § 63,

$$2a_3 = 2^2 - 3 + 1, \text{ or } a_3 = 1 .$$

Then by (4)

$$a_1 = 2^{n-2} + 2^{n-4} + \ldots + 2^3 + 2 .$$

The condition is thus

$$a_1^{2^{n-2}+\ldots+2^3+2} a_3 = 0 .$$

Hence would $a_3 = 0$. But $\xi^4 + a_1\xi^3$ vanishes for $\xi = a_1$. Hence $a_1 \neq 0$ leads to no substitution quantic.

Our quantic thus becomes

$$\xi^4 + a_2\xi^2 + a_3\xi$$

which is suitable on 2^n letters if and only if a determinant of the form (3) in § 58 is $\neq 0$.

72. $p^r = 5$.

Cases depending on which is the first coefficient $\neq 0$.

(a) ξ^5.

Suitable on 5^n letters by § 18.

(b) $\xi^5 + a_4\xi$, $a_4 \neq 0$.

Suitable by corollary to § 57 if $-a_4$ is a not fourth power in the $GF[5^n]$.

(c) $\xi^5 + a_3\xi^2 + a_4\xi$, $a_3 \neq 0$.

Rejected by § 66.

(d) $\xi^5 + a_2\xi^3 + a_4\xi$, $a_2 \neq 0$.

The coefficient of ξ^2 has been removed by a linear transformation. The lowest power giving a condition is

$$5^{n-1} + 2 \cdot 5^{n-2} + 2 \cdot 5^{n-3} + \ldots + 2 \cdot 5 + 3 .$$

Thus $g = 2$ or $3 = E\left[\frac{5+1}{2}\right]$, since $g > 1$ by § 64.

For $g = 2$, $a_4 = 1$, $a_2 = 5^{n-1} + 5^{n-2} + \ldots + 5 + 1$;

for $g = 3$, $a_4 = 0$, $a_2 = 5^{n+1} + 5^{n-2} + \ldots + 5 + 3$.

The condition is thus (using § 15)

$$2^{n-2} \cdot 3!\, a_2^{5^{n-1}+\ldots+5+1} a_4 + 2^{n-2} a_2^{5^{n-1}+\ldots+5+3} = 0$$

or

$$a_4 = 4a_2^2 .$$

The quintic is thus $\xi(\xi^2 - 2a_2)^2$, which is indeed suitable on the 5^n marks of the $GF[5^n]$, if $2a_2$ be a not-square in the field. For if, when $\eta \neq \varphi$,

$$\eta(\eta^2 - 2a_2)^2 = \varphi(\varphi^2 - 2a_2)^2$$

on dividing out $\eta - \varphi$,

$$(\eta - \varphi)^4 + a_2(\eta^2 + \eta\varphi + \varphi^2) + 4a_2^2 = 0 .$$

Substituting

$$\eta = \lambda + \mu , \quad \varphi = \lambda - \mu ,$$

$$(\mu^2 - 2a_2)^2 = 2a_2\lambda^2 .$$

(e) The case $a_1 \neq 0$ is rejected by § 65.

73. $p^r = 7$.

(a) ξ^7 is suitable on 7^n letters.

(b) $\xi^7 + a_6\xi$.

Suitable if $-a_6$ is a not-sixth power in the $GF[7^n]$.

(c) $\xi^7 + a_5\xi^2$, $a^5 \neq 0$.

Consider the power

$$a_0 + a_5 = 2 \cdot 7^{n-1} + 4\,(7^{n-2} + 7^{n-3} + \ldots + 7) + 5\,.$$

If $7a_0 + 2a_5 = 2\,(7^n - 1)$, then we find

$$a_5 = 6 \cdot 7^{n-2} + 3 \cdot 7^{n-3} + \ldots$$

contrary to the method of partition required by § 14.

If $7a_0 + 2a_5 = 7^n - 1$, we find

$$a_0 = 2 \cdot 7^{n-2} + 2 \cdot 7^{n-3} + \ldots + 2 \cdot 7 + 2\,;\; a_5 = 2 \cdot 7^{n-1} + 2 \cdot 7^{n-2} + \ldots + 2 \cdot 7 + 3.$$

Hence $a_5 = 0$.

(d) $\xi^7 + a_4\xi^3 + a_5\xi^2 + a_6\xi$.

Rejected by § 66.

(e) $\xi^7 + a_3\xi^4 + a_5\xi^2 + a_6\xi$, $a_3 \neq 0$.

For the power $7^{n-1} + 3\,(7^{n-2} + \ldots + 7) + 4$, $g = 2$ giving

$$a_3{}^{7^{n-1}+\ldots+7+1}\, a_5 = 0, \text{ or } a_5 = 0\,.$$

For the power $7^{n-1} + 3\,(7^{n-2} + \ldots + 7) + 5$, $g = 3$, 4, or 5, giving

$$(3!)^{n-2} \cdot 5! \left\{ \frac{a_3{}^{7^{n-1}+\ldots+7+1}\, a_6{}^2}{2^n} + \frac{a_3{}^{7^{n-1}+\ldots+7+3} a_6}{2^{n-2} \cdot 3!} + \frac{a_3{}^{7^{n-1}+\ldots+7+5}}{2^{n-2} \cdot 5!} \right\} = 0\,,$$

or

$$a_3{}^{7^{n-1}+\ldots+7+1}\,(a_6 - 2a_3{}^2)^2 = 0\,.$$

The only possible form is thus

$$\xi\,(\xi^3 - 3a_3)^2\,.$$

(f) $\xi^7 + a_2\xi^5 + a_4\xi^3 + a_5\xi^2 + a_6\xi$, $a_2 \neq 0$.

The power $7^{n-1} + 2 \cdot 7^{n-2} + 2 \cdot 7^{n-3} + \ldots + 2 \cdot 7 + 3$ requires

$$2^{n-2} \cdot 3!\{\tfrac{1}{2}\, a_2{}^{7^{n-1}+\ldots+7+2}\, a_4 + \tfrac{1}{2}\, a_2{}^{7^{n-1}+\ldots+7}\, a_4{}^2 + a_2{}^{7^{n-1}+\ldots+7+1}\, a_6\} = 0$$

or

$$a_2{}^2 a_4 + a_4{}^2 + 2a_2 a_6 = 0\,. \tag{1}$$

The power $7^{n-1} + 2 \cdot 7^{n-2} + 2 \cdot 7^{n-3} + \ldots + 2 \cdot 7 + 4$ requires

$$2^{n-2} \cdot 4!\, a_2{}^{7^{n-1}+\ldots+7}\, a_5\{\tfrac{1}{6}\, a_5{}^2 + a_4 a_6 + \tfrac{1}{2}\, a_2 a_4{}^2 + \tfrac{1}{2}\, a_2{}^2 a^6\} = 0\,.$$

(Thus $g < 7 = E\left[\frac{2 \cdot 7 + 1}{2}\right]$; so that by the partition requirements we have from (4) § 63 that $g \leqq h$ or 4.)

Applying (1), either $a_5 = 0$ or else

$$a_2^2 a_5^2 = - a_2 a_4 (3a_2^2 + 5a_4)^2 \tag{2}$$

and thus $- a_2 a_4$ would be a square in the $GF[7^n]$.

Consider the power $2 \cdot 7^{n-1} + 2 \cdot 7^{n-2} + \ldots + 2 \cdot 7 + 2$.

For $s = 2(7^n - 1)$, we apply § 67 for $q = h = k = 2$, $t = 0$. Hence

$$g = 1, \; a_4 = a_5 = a_6 = 0, \; a_0 = a_2 = 7^{n-1} + 7^{n-2} + \ldots + 7 + 1 .$$

The coefficient of $\xi 2(7^n - 1)$ is thus $2^n a_2^{7^{n-1}+\ldots+7+1}$.

For $s = 7^n - 1$, we have

$$a_0 + a_2 + a_4 + a_5 + a_6 = 2(7^{n-1} + \ldots + 7 + 1)$$

$$7a_0 + 5a_2 + 3a_4 + 2a_5 + a_6 = 6(7^{n-1} + \ldots + 7 + 1) = 7^n - 1 .$$

Hence

$$4a_0 + 2a_2 - a_5 - 2a_6 = 0 .$$

Using the notation

$$a_i = \sum_{j=0}^{n-1} c_j^{(i)} \cdot 7^j \qquad (i = 0, 2, 4, 5, 6)$$

we know by § 14 that each $c_j^{(i)}$ is 0, 1, or 2 such that

$$c_j^{(0)} + c_j^{(2)} + c_j^{(4)} + c_j^{(5)} + c_j^{(6)} = 2 . \quad (j = 0, 1, \ldots, n-1)$$

We have immediately

$$4c_0^{(0)} + 2c_0^{(2)} - c_0^{(5)} - 2c_0^{(6)} = 7m$$

m being an integer. But m must be zero. By induction,

$$4c_j^{(0)} + 2c_j^{(2)} - c_j^{(5)} - 2c_j^{(6)} = 0 . \quad (j = 0, 1, \ldots, n-1)$$

Then $c_j^{(5)} = 0$ or 2. But if $c_j^{(5)} = 2$, $c_j^{(0)} = c_j^{(2)} = c_j^{(6)} = 0$ and the last equation is not satisfied. Finally, $c_j^{(0)} = 0$. Hence $a_0 = a_5 = 0$ and $a_2 = a_6$. Then

$$2a_2 + a_4 = 2(7^{n-1} + \ldots + 7 + 1)$$

from which it follows that a_2 takes exactly the 2^n values

$$\sum_{j=0}^{n-1} c_j^{(2)} \cdot 7^j$$

where $c_j^{(2)} = 0$ or 1. We thus obtain 2^n terms,

$$(a_2\xi^5)^{a_2}\ (a_4\xi^3)^{a_4}\ (a_6\xi)^{a_2}$$

or

$$(a_2a_6)^{a_2}\ (a_4^2)^{7^{n-1}+7^{n-2}+\ldots+7+1-a_2}\,.$$

Hence, as far as their literal parts, these 2^n terms are identical with those given by the expansion

$$(2a_2a_6 + a_4^2)^{7^{n-1}+7^{n-2}+\ldots+7+1}\,.$$

In order that the numerical coefficients be congruent modulo 7, we must have by § 15,

$$2^{a_2} = 2^n \Big/ \prod_{j=0}^{n-1} (c_j^{(4)}!)$$

But if l of the $c_j^{(2)}$'s are $= 1$, l of the $c_j^{(4)}$'s are zero and hence $n - l$ are $= 2$. Hence

$$\prod_{j=0}^{n-1} (c_j^4!) = 2^{n-l}\,.$$

$$2^{a_2} = \prod_{j=0}^{n-1} (2^{7^j})^{c_j^{(2)}} = \prod_{j=0}^{n-1} (2)^{c_j^{(2)}} = 2^l\,.$$

The identification is thus complete.

The complete condition given by the above power is thus

$$2^n a_2^{7^{n-1}+\ldots+7+1} + (2a_2a_6 + a_4^2)^{7^{n-1}+\ldots+7+1} = 0\,.$$

Applying (1) and remembering that $a_2 \neq 0$,

$$(-a_2a_4)^{(7^n-1)/6} = -2^n\,. \tag{3}$$

Hence

$$(-a_2a_4)^{(7^n-1)/2} = -(2^3)^n = -1\,,$$

so that $-a_2a_4$ is a not-square in the $GF[7^n]$. Hence by (2) $a_5 = 0$.

The power $7^{n-1} + 2\,.\,7^{n-2} + 2\,.\,7^{n-3} + \ldots + 2\,.\,7 + 5$ requires

$$a_2^{7^{n-1}+7^{n-2}+\ldots+7^2}\{2a_4^9 + 4a_2a_4^7a_6 + 6a_2^2a_4^8 + a_2^4a_4^7 + 4a_2^7a_4a_6^3 + a_2^7a_4^4a_6 + 6a_2^8a_4^2a_6^2 + 2a_2^9a_6^3 + 2a_2^{15}a_6 + a_2^{14}a_4^2 + 3a_2^{16}a_4 + 4a_2^{18}\} = 0\,,$$

the last four terms not occurring when $n = 2$.

Applying (1) to eliminate a_6,

$$4a_4^8 + 4a_2^2a_4^7 + a_2^4a_4^6 + 2a_2^6a_4^5 + 2a_2^8a_4^4 + 5a_2^{10}a_4^3 + 2a_2^{14}a_4 + 4a_2^{16} = 0\,, \tag{4}$$

the last two terms not occurring when $n = 2$.

For $n = 2$, we may give (4) the form

$$4a_4^3(a_4 - 2a_2^2)(a_4 - 4a_2^2)(a_4 - 5a_2^2)[a_4 - (1 + \sqrt{3})a_2^2][a_4 - (1 - \sqrt{3})a_2^2] = 0.$$

But by (3)

$$(a_2a_4)^8 = -2^2 = 3.$$

Hence a_2 is a not-square in the $GF[7^2]$ and

$$a_4 = \pm 2a_2^2.$$

Thus $(\pm 2)^8 = 4$; $4^8 = 2$; $(1 \pm \sqrt{3})^8 = 5$, each modulo 7.

For $n > 2$, (4) may be written

$$4(a_4 + 2a_2^2)^5(a_4^3 - 2a_4^2a_2^2 + 3a_4a_2^4 + 2a_2^6) = 0, \qquad (4')$$

the last factor being irreducible in the $GF[7^1]$.

By using § 68, I find that the power

$$7^{n-1} + 2 \cdot 7^{n-2} + \ldots + 2 \cdot 7^2 + 3 \cdot 7 + 2$$

gives for $n > 2$ a condition of six terms which on applying (1) to eliminate a_6 reduces to an identity. But the power $7^{n-1} + 2 \cdot 7^{n-2} + \ldots + 2 \cdot 7^2 + 3 \cdot 7 + 4$ requires for $n > 2$

$$\begin{aligned} a_2^{7^{n-1}+\cdots+7^2}\{&4a_2a_6^8a_4^7 + 2a_6^7a_4^9 + 4a_2^2a_6^7a_4^8 + 6a_2^7a_6^{10}a_4 + 5a_2^4a_6^7a_4^7 + 3a_6^3a_4^{15} \\ &+ 2a_2^{15}a_6^8 + a_2^{14}a_6^7a_4^2 + 2a_2^8a_6a_4^{14} + a_2^7a_4^{16} + 2a_2^{16}a_6^7a_4 + 2a_2^9a_4^{15} \\ &+ 6a_2^{18}a_6^7 + 3a_2^{14}a_6^3a_4^8 + 6a_2^{11}a_4^{14}\} = 0. \end{aligned}$$

Applying (1) to eliminate a_6 (the 4th, 6th and 14th terms cancel),

$$a_4^7\{6a_4^{15} + a_2^2a_4^{14} + 3a_2^{14}a_4^8 + 4a_2^{16}a_4^7 + 3a_2^{28}a_4 + 4a_2^{30}\} = 0,$$

or

$$a_4^7(a_4 + 6a_2^2)(a_4 + 2a_2^2)^{14} = 0.$$

Hence by (4') the only possible values, when $n > 2$, are

$$a_4 = -2a_2^2, \quad a_6 = -a_2^3.$$

The same holds also for $n = 2$, since the set of values

$$a_4 = +2a_2^2, \quad a_6 = 4a_2^3$$

is excluded by the condition, given by the 18th power,

$$\begin{aligned} a_2a_4^7 + 3a_2^7a_4a_6^2 + 5a_2^9a_6^2 + 3a_2^8a_4^2a_6 + 2a_2^7a_4^4 + 4a_2^{15} + 3a_2a_4^7a_6^8 \\ + 5a_4^9a_6^7 + 3a_2^2a_4^8a_6^7 + a_2^7a_4a_6^{10} + 2a_2^4a_4^7a_6^7 + 4a_4^{15}a_6^3 = 0, \end{aligned}$$

which reduces to $6a_2^{15} = 0$ by substituting the latter set of values, is an identity for

$$a_4 = -2a_2^2, \quad a_6 = -a_2^3.$$

The only possible form is thus $\xi(\xi^2 - 2a_2)^3$, which may be proved suitable on 7^n letters, if $2a_2$ be a not-square, by the method used in § 39 or as below.

74. $p^r = 11$.

(a) $\xi^{11} + a_{10}\xi$.

Suitable if $-a_{10}$ be a not-tenth power in the $GF[11^n]$.

(b) $\xi^{11} + a_9\xi^2$, $a_9 \neq 0$.

The power $3 \cdot 11^{n-1} + 7(11^{n-2} + \ldots + 11) + 9$ requires $a_9 = 0$.

(c) $\xi^{11} + a_8\xi^3 + a_{10}\xi$, $a_8 \neq 0$.

For the power $2 \cdot 11^{n-1} + 6(11^{n-2} + \ldots + 11) + 8$, we must have $s = 11^n - 1$ and then $a_0 \leqq 6(11^{n-2} + \ldots + 11) + 8$. We may prove by induction that

$$a_0 \leqq 4(11^{n-2} + 11^{n-3} + \ldots + 11) + 8.$$

Thus suppose

$$a_0 = 4(11^{n-2} + 11^{n-3} + \ldots + 11^{n-k}) + 6(11^{n-k-1} + \ldots + 11) + 8 - x,$$

$$0 \leqq x \leqq 11^{n-k-1} + 6(11^{n-k-2} + \ldots + 11) + 8.$$

Then

$$a_8 + a_{10} = 2 \cdot 11^{n-1} + 2 \cdot 11^{n-2} + \ldots + 2 \cdot 11^{n-k} + x.$$

If $a_8 = 2 \cdot 11^{n-1} + \ldots + 2 \cdot 11^{n-k} + y$, where $0 \leqq y \leqq x$,

$$s = 11^n + 11^{n-k} + 6(11^{n-k-1} + \ldots + 11^2) + 8 \cdot 11 - 10x + 2y > 11^n.$$

If $a_8 = 2 \cdot 11^{n-1} + \ldots + 2 \cdot 11^{n-k+1} + 11^{n-k} + y$,

$$s = 10(11^{n-1} + \ldots + 11^{n-k+1} + 11^{n-k}) + 6(11^{n-k-1} + \ldots + 11^2) + 8 \cdot 11 - 10x + 2y < 11^n - 1.$$

Hence

$$a_0 < 4(11^{n-2} + \ldots + 11^{n-k}) + 5 \cdot 11^{n-k-1}$$

and thus

$$\leqq 4(11^{n-2} + \ldots + 11^{n-k-1}) + 6(11^{n-k-2} + \ldots + 11) + 8.$$

It is now easily shown that

$$a_0 = 4(11^{n-2} + \ldots + 11 + 1), \quad a_8 = 2 \cdot 11^{n-1} + \ldots + 2 \cdot 11 + 3, \quad a_{10} = 1,$$

as a smaller value for a_0 would require $s < 11^n - 1$. The condition is thus

$$a_8^{2 \cdot 11^{n-1} + \ldots + 2 \cdot 11 + 3} a_{10} = 0 \text{ or } a_{10} = 0.$$

The power $2\,.11^{n-1} + 6(11^{n-2} + \ldots + 11) + 10$ then requires that $a_8 = 0$.

(d) $\xi^{11} + a_7\xi^4 + a_9\xi^2 + a_{10}\xi$, $a_7 \neq 0$.

The powers $11^{n-1} + 7(11^{n-2} + \ldots + 11) + 9$, $11^{n-1} + 7(11^{n-2} + \ldots + 11) + 10$, and $2\,.\,11^{n-1} + 4(11^{n-2} + \ldots + 11) + 8$, require in turn,

$$a_9 = 0\,, \quad a_{10} = 0\,, \quad a_7 = 0\,.$$

(e) $\xi^{11} + a_6\xi^5 + \ldots$ is rejected by § 66.

(f) $\xi^{11} + a_5\xi^6 + a_7\xi^4 + a_8\xi^3 + a_9\xi^2 + a_{10}\xi$, $a_5 \neq 0$.

The power $11^{n-1} + 5(11^{n-2} + \ldots + 11) + 6$ requires $a_7 = 0$.

The powers $11^{n-1} + 5(11^{n-2} + \ldots + 11) + 7$ and $11^{n-1} + 5(11^{n-2} + \ldots + 11^2) + 6\,.\,11 + 4$ require respectively

$$a_5{}^{11^{n-1}+\ldots+11+1}(a_9{}^2 + 2a_8a_{10} + 5a_5{}^2a_8) = 0$$

$$a_5{}^{11^{n-1}+\ldots+11+1}a_8{}^{11}(a_9{}^2 + 2a_8a_{10} + 4a_5{}^2a_8) = 0\,.$$

Hence $a_8 = 0$ and then $a_9 = 0$.

The power $11^{n-1} + 5(11^{n-2} + \ldots + 11) + 9$ of $\xi^{11} + a_5\xi^6 + a_{10}\xi$ requires

$$a_5{}^{11^{n-1}+\ldots+11+1}(a_{10} - 3a_5{}^2)^4 = 0\,.$$

The only possible form is thus $\xi(\xi^5 - 5a_5)^2$.

(g) The cases $a_2 \neq 0$, $a_3 \neq 0$, $a_4 \neq 0$ I have not attempted. $a_1 = 0$ by § 65.

75. Theorem.* *If d be any divisor of $p^r - 1$, the quantic*

$$\xi(\xi^d - \nu)^{(p^r-1)/d}\,,$$

where ν is a not dth power in the $GF[p^n]$, represents a substitution on its p^n marks.

We are to show that

$$\xi(\xi^d - \nu)^{(p^r-1)/d} = \beta \tag{1}$$

has a solution ξ belonging to the $GF[p^n]$, β being an arbitrary mark of that field. The statement being evident when $\beta = 0$, we will suppose that $\beta \neq 0$. Writing $\varphi = \xi^d - \nu$ our quantic becomes

$$\varphi^{(p^r-1)/d}\,.\,(\varphi + \nu)^{1/d} \equiv (\varphi^{p^r} + \nu\varphi^{p^r-1})^{1/d}\,.$$

It is then sufficient to prove that

$$\varphi^{p^r} + \nu\varphi^{p^r-1} = \beta^d = \delta \tag{2}$$

* From the results of §§ 70, 72, 73, and 74, for $p = 3$, 5, 7 and 11, respectively, I venture the conjecture that all substitution quantics of degree p suitable on p^n letters are reducible to the simple type

$$\xi(\xi^d - \nu)^{(p-1)/d}$$

where d is a divisor of $p - 1$.

has a solution φ belonging to the $GF[p^n]$, δ being any dth power and ν any not dth power of the field. For if there be such a solution φ (which $\neq 0$, since $\beta \neq 0$), then

$$\xi = (\varphi + \nu)^{1/d} = \beta/\varphi^{(p^r-1)/d}$$

will belong to the $GF[p^n]$ and satisfy (1).

Writing in (2)

$$\varphi = 1/\omega$$

and multiplying by ω^{p^r}, we obtain

$$1 + \nu\omega = \delta\omega^{p^r}.$$

If we make

$$\delta\delta' = 1, \quad \nu\delta' = \nu',$$

δ' being thus a dth power and ν' a not dth power in the field, the last equation becomes

$$\omega^{p^r} - \nu'\omega = \delta'.$$

But this always has a solution in the field; for by § 57, corollary, the quantic

$$\omega^{p^r} - \nu'\omega$$

represents a substitution on p^n letters, ν' being a not dth power and hence a not $(p^r - 1)$st power, d being a divisor of $p^r - 1$.

For $r = n$, this theorem is a special case of the following theorem:*

76. *If r is prime to and $< p^n - 1$, if s is a divisor of $p^n - 1$, and if $f(\xi^s)$ is a rational integral function of ξ^s belonging to the $GF[p^n]$ which can never vanish, then the quantic*

$$\xi^r [f(\xi^s)]^{(p^n-1)/s}$$

represents a substitution on p^n letters.

For if the quantic be raised to the lth power, l being not divisible by s, we have a set of terms whose exponents are of the form $ms + lr$ and thus are not divisible by s and hence not by $p^n - 1$. But if

$$l = ts < p^n - 1,$$

we get the term ξ^{lr}, since by the hypothesis on $f(\xi^s)$ we have

$$[f(\xi^s)]^{p^n-1} = 1.$$

But lr is not divisible by $p^n - 1$.

* Proved for $n = 1$ by Rogers, l. c. p. 41. I give a modified proof.

77. The substitution quantics given by § 76 and, when $n \leqq r$, by § 75 are not reduced.

Thus, for $p > 2$, we have the suitable quantic

$$\xi^r (\xi^{\frac{p^n-1}{2}} - \nu)^2 = -2\nu\{\xi^{\frac{p^n-1}{2}+r} - 1/2\,(\nu + 1/\nu)\,\xi^r\}$$

ν being a not $(p^n - 1)/2$ power in the $GF[p^n]$ and thus any mark except $+1, -1, 0$. For the $p^n - 3$ values of ν, we get for each value of r, $(p^n - 3)/2$ different substitution quantics on p^n letters. For if

$$\nu + 1/\nu = \nu' + 1/\nu'$$

then either $\nu = \nu'$ or $\nu = 1/\nu'$. Also $\nu \neq 1/\nu$.

Examples of the above quantic:

$n = 1,\ p = 5$: ξ^3 and ξ.

$n = 1,\ p = 7$: $\xi^4 \pm 3\xi$ and $\xi_5 \pm 2\xi^2$, Hermite's forms.

$n = 1,\ p = 11$: $\xi^6 \pm 2\xi$, $\xi^6 \pm 4\xi$ (see § 45).

$n = 2,\ p = 3$: ξ, ξ^3, ξ^5, $\xi^5 \pm 2^{1/2}\xi$ (see § 44).

For the values $n = 1, p = 7$, we have if $\nu^3 = -1$,

$$\xi\,(\xi^2 - \nu)^3 = -3\nu\,(\xi^5 - \nu\xi^3 + 3\nu^2\xi)$$

$$\xi^5\,(\xi^2 - \nu)^3 = 2\,\{\xi^5 + 2\nu\xi^3 + 3\,(2\nu)^2\xi\}$$

which together give the known quantic on 7 letters,

$$\xi^5 + a\xi^3 + 3a^2\xi\,, \qquad a = \text{arbitrary}.$$

SECTION IV.—*Degree a multiple, but not a power, of p.*

78. Attempting no general investigation, I will confine myself to the determination of all *sextics* suitable on 3^n letters, together with a few special results on *sextics* suitable on 2^n letters.

$\varphi(\xi) = \xi^6 + a_1\xi^5 + a_2\xi^4 + a_3\xi^3 + a_4\xi^2 + a_5\xi$ *on* 3^n *letters*, §§ 79–82

79. Applying a linear transformation (in the $GF[3^n]$),

$$\varphi(\xi + \eta) = \xi^6 + a_1\xi^5 + (a_2 + 2a_1\eta)\,\xi^4 + (a_3 + a_2\eta + a_1\eta^2 + 2\eta^3)\,\xi^3$$
$$+ (a_4 + a_1\eta^3)\,\xi^2 + (a_5 + 2a_4\eta + a_2\eta^3 + 2a_1\eta^4)\,\xi + \varphi(\eta)\,.$$

Hence if $a_1 \neq 0$, either the coefficient of ξ^4 or that of ξ^2 can be removed by choice of η. But if $a_1 = 0$, no other coefficient can be removed in general by a linear transformation.

80. The case $a_1 = 0$.

(a) $n = 2$.

The second, fourth and fifth powers require respectively,

$$a_4 = a_2^2 \tag{1}$$

$$1 + a_2^4 + a_4^4 = 0 \tag{2}$$

$$a_2^3 + 2a_2a_4 + a_2^3 + 2a_3^3a_5 + 2a_2^3a_3a_5 + a_2^3a_4^2 + 2a_2a_3^4 + 2a_2a_5^4 + 2a_2a_4^3 + 2a_3a_4a_5^3 + a_4^3a_5^2 = 0 . \tag{3}$$

The seventh power requires exactly the cube of (3).

From (1) and (2), a_2 is a square $\neq 0$ in the $GF[3^2]$.

From (1) and (3),

$$(a_3^2 + 2a_2^3a_3a_5 + a_2^6a_5^2) + 2(a_5 + a_2a_3)(a_3^3 + a_2a_5^3) = 0 .$$

Multiplying by a_2^3 and applying $a_2^4 = 1$,

$$(a_5 + a_2a_3)^2\{a_2 + 2(a_5 + a_2a_3)^2\} = 0 .$$

Hence either

$$a_5 = 2a_2a_3 \text{ or } a_5 = 2a_2a_3 \pm a_2^{1/2} .$$

The case $a_5 = 2a_2a_3$ is excluded below. The quantic

$$\xi^6 + a_2\xi^4 + a_3\xi^3 + a_2^2\xi^2 + (2a_2a_3 \pm a_2^{5/2})\xi \tag{4}$$

becomes by writing $\xi = \pm a_2^{1/2}\eta$, $a_3 = \pm a_2^{3/2}a$,

$$a_2^3\{\eta^6 + \eta^4 + a\eta^3 + \eta^2 + (2a + 1)\eta\} .$$

The resultant of the equations

$$\eta^6 + \eta^4 + a\eta^3 + \eta^2 + (2a + 1)\eta = 0 ; \ \eta^8 = 1$$

is

$$a^5 - a^4 + a^2 + 1 = (a + 1)(a^2 - a - 1)^2 .$$

Hence a may have any value in the $GF[3^2]$ except 2 and $2 \pm 2^{1/2}$.

The ultimately reduced form of (4)

$$\xi^6 + \xi^4 + a\xi^3 + \xi^2 + (2a + 1)\,\xi$$

represents the following substitutions on the marks of the $GF[3^2]$:

(0) (1) (-1) $(2^{1/2}, 2^{1/2} - 1, 2^{1/2} + 1)$ $(-2^{1/2}, -2^{1/2} - 1, -2^{1/2} + 1)$ for $a = 0$.

(0) (1) (-1) $(2^{1/2}, -2^{1/2} - 1, 2^{1/2} + 1, -2^{1/2}, 2^{1/2} - 1, -2^{1/2} + 1)$ for $a = 1$.

(0) (1) (-1) $(-2^{1/2})$ $(-2^{1/2} + 1)$ $(-2^{1/2} - 1)$ $(2^{1/2}, 2^{1/2} + 1, 2^{1/2} - 1)$ for $a = 2^{1/2}$.

(0) (1) (-1) $(2^{1/2}, -2^{1/2} + 1, 2^{1/2} + 1, -2^{1/2} - 1, 2^{1/2} - 1, -2^{1/2})$ for $a = 1 + 2^{1/2}$.

(b) $n > 2$. Write $3^n = 6m + 3$, m being thus of the form $9k + 4$. The powers $m + 1$, $m + 3$, and $m + 4$ require respectively

$$a_4 = a_2^2 \tag{1}$$

$$a_4 (2a_4^3 + a_2^6) = 0$$

$$a_2a_5^4 + a_3a_4a_5^3 + 2a_4^3a_5^2 + a_2^3a_4^4 + 2a_3^6a_4 + a_2^6a_2^5 + 2a_2^5a_4^3 + a_2^4a_3^3a_5 + a_2^3a_3^4a_4 + a_2^2a_3^6 + 2a_2^9a_4 + a_2^{11} = 0\,, \tag{2}$$

the last two terms not occurring when $n = 3$.

Applying (1) to (2), we have whether $n \gtrless 3$,

$$a_2 (a_5^4 + a_2a_3a_5^3 + a_2^3a_3^3a_5 + a_2^4a_3^4) = a_2 (a_5 + a_2a_3)^4 = 0\,.$$

Consider the power $3^{n-1} + 3^{n-2} + \ldots + 3 + 1 = a_0 + a_2 + a_3 + a_4 + a_5$. For $s = 6a_0 + 4a_2 + 3a_3 + 2a_4 + a_5 = 3(3^n - 1)$, we have

$$a_0 = 3^{n-1} + \ldots + 3 + 1\,, \quad a_2 = a_3 = a_4 = a_5 = 0\,.$$

For $6a_0 + 4a_2 + 3a_3 + 2a_4 + a_5 = 2(3^n - 1) = 3^n + 2 \cdot 3^{n-1} + 2 \cdot 3^{n-2} + \ldots + 2 \cdot 3 + 1$, it follows that $a_4 = 0$. For, in the notation of § 73 (f), if $c_j^{(4)} = 1$, then $c_{j+1}^{(4)} = 1, \ldots c_{n-1}^{(4)} = 1$; while $a_4 > 3^{n-1}$ would give $s < 2(3^n - 1)$. Also $a_5 = 0$; for if $c_r^{(5)} = 1$, then $c_{r+1}^{(4)} = 1$.

Thus $2a_0 - a_3 = 0$, or $a_0 = a_3 = 0$, $a_2 = 3^{n-1} + \ldots + 3 + 1$.

For $s = 3^n - 1$, we have at once

$$a_4 = 3^{n-1} + 3^{n-2} + \ldots + 3 + 1\,, \quad a_0 = a_2 = a_3 = a_5 = 0\,.$$

The condition is thus

$$1 + a_2^{3^{n-1}+\ldots+3+1} + a_4^{3^{n-1}+\ldots+3+1} = 0 .$$

Hence by (1), a_2 is a square $\neq 0$ in the $GF[3^n]$.

The only possible form is thus

$$\xi^6 + a_2\xi^4 + a_3\xi^3 + a_2^2\xi^2 + 2a_2a_3\xi ,$$

which is *not* suitable on 3^n letters since it vanishes for $\xi = a_2^{1/2} \neq 0$.

81. The case $a_1 \neq 0$. Removing the term a^4, we consider

$$\xi^6 + a_1\xi^5 + a_3\xi^3 + a_4\xi^2 + a_5\xi .$$

(a) $n = 2$. The second, fourth and fifth powers require respectively,

$$a_4 = 2a_1a_3 . \tag{1}$$

$$1 + a_1^3a_5 + a_1a_5^3 + a_4^4 = 0 . \tag{2}$$

$$a_3^2 + 2a_1a_5 + 2a_1^3a_3 + 2a_3^3a_5 + a_1^2a_4^3 + 2a_1a_3^3a_4 + 2a_3a_4a_5^3 + a_4^3a_5^2 = 0 . \tag{3}$$

The seventh power requires the cube of (3).

First, $a_4^8 = 1$. For if $a_4 = 0$, then $a_3 = 0$ by (1) and then $a_5 = 0$ by (3), which is contrary to (2).

By squaring (2),

$$a_1^6a_5^2 + 2a_1^4a_5^4 + a_1^2a_5^6 = a_4^8 + 2a_4^4 + 1 = 2(a_4^4 + 1)$$
$$= a_1^3a_5 + a_1a_5^3 . \tag{2'}$$

But $a_5 \neq 0$; for if $a_5 = 0$, then by (3)

$$a_1^6(a_3^2 + 2a_1^3a_3 + 2a_1^5a_3^3 + a_1^2a_3^4) = a_3(a_3 - a_1^3)(a_3^2 + a_1^6) = 0 .$$

If either $a_3 = a_1^3$ or $a_3 = 2^{1/2}a_1^3$, then by (1) $a_4^4 = 1$, contrary to (2) for $a_5 = 0$.

Hence by (2')

$$a_1^5a_5 + 2a_1^3a_5^3 + a_1a_5^5 + 2a_1^2 + 2a_5^2 = 0 .$$

Writing $a_5 = \eta a_1^5$ this becomes, aside from the factor a_1^2,

$$(\eta + 1)(\eta^2 + 1)(\eta^2 - \eta - 1) = 0 .$$

If $\eta = -1$, $\alpha_4^4 = 1$ by (2), while (3) becomes

$$\alpha_1^6 + 2\alpha_1^3\alpha_3 + 2\alpha_1^5\alpha_3^3 + \alpha_1^2\alpha_3^4 = \alpha_1^2(\alpha_3 - \alpha_1^3)^4 = 0.$$

The resulting quantic

$$\xi^6 + \alpha_1\xi^5 + \alpha_1^3\xi^3 - \alpha_1^4\xi^2 - \alpha_1^5\xi$$

is suitable on 3^2 letters. Thus for $\alpha_1 = 1$, it represents the following substitution on the marks of the $GF[3^2]$:

$$(0)(1)(-1)(2^{1/2}, -2^{1/2})(2^{1/2}+1, -2^{1/2}-1, -2^{1/2}+1, 2^{1/2}-1).$$

If $\eta^2 = -1$, $\alpha_5 = 2^{1/2}\alpha_1^5$, while (2) and (3) become

$$\alpha_4^4 = -1;$$

$$(1 - 2^{1/2})\alpha_3^2 - 2^{1/2}\alpha_1^6 + 2\alpha_1^3\alpha_3 - 2^{1/2}\alpha_3^3\alpha_1^5 + \alpha_1^2\alpha_3^4 = 0.$$

Multiplying by α_1^2, and placing $\alpha_1^4\alpha_3^4 = \alpha_4^4 = -1$, $\alpha_3 = \varphi\alpha_1^3$,

$$-2^{1/2}\varphi^3 + (1 - 2^{1/2})\varphi^2 + 2\varphi - (1 + 2^{1/2}) = 0,$$

whose roots are

$$1 - 2^{1/2}, \quad -1 - 2^{1/2}, \quad -1 + 2^{1/2}.$$

But $\xi^6 + \alpha_1\xi^5 + \varphi\alpha_1^3\xi^3 - \varphi\alpha_1^4\xi^2 + 2^{1/2}\alpha_1^5\xi$ vanishes for $\xi = -2^{1/2}\alpha_1$ when $\varphi = -1 - 2^{1/2}$, while for $\varphi = 1 - 2^{1/2}$ or $\varphi = -1 + 2^{1/2}$ it represents a substitution on the marks of the $GF[3^2]$. Thus, taking $\alpha_1 = 1$,

$$\xi^6 + \xi^5 + (1 - 2^{1/2})\xi^3 - (1 - 2^{1/2})\xi^2 + 2^{1/2}\xi,$$

$$\xi^6 + \xi^5 + (-1 + 2^{1/2})\xi^3 - (-1 + 2^{1/2})\xi^2 + 2^{1/2}\xi,$$

represent respectively the substitutions

$$(0)(-1, 2^{1/2}+1)(1, 2^{1/2}-1, -2^{1/2}, -2^{1/2}-1, 2^{1/2}, -2^{1/2}+1)$$

$$(0)(-1)(1, 2^{1/2}-1, 2^{1/2})(2^{1/2}+1, -2^{1/2}, -2^{1/2}+1, -2^{1/2}-1).$$

If $\eta^2 = \eta + 1$, $\alpha_5 = (2^{1/2} - 1)\alpha_1^5$, and (2) and (3) become

$$\alpha_4^4 = 1$$

$$-2^{1/2}\alpha_3^2 + (1 - 2^{1/2})\alpha_1^6 + 2\alpha_1^3\alpha_3 + 2^{1/2}\alpha_1^5\alpha_3^3 + \alpha_1^2\alpha_3^4 = 0.$$

Multiplying by α_1^2 and placing $\alpha_1^4\alpha_3^4 = \alpha_4^4 = 1$, $\alpha_3 = \varphi\alpha_1^3$

$$2^{1/2}\varphi^3 - 2^{1/2}\varphi^2 - \varphi - (2^{1/2} + 1) = 0 .$$

Its roots are -1, $1 \pm (-2^{1/2} - 1)^{1/2}$, of which the last two are not marks of the $GF[3^2]$ since $(-2^{1/2} - 1)^4 = -1$.

The quantic given by $\varphi = -1$,

$$\xi^6 + \alpha_1\xi^5 - \alpha_1^3\xi^3 + \alpha_1^4\xi^2 + (2^{1/2} - 1)\,\alpha_1^5\xi$$

represents when $\alpha_1 = 1$ the substitution on the marks of the $GF[3^2]$:

$$(0)\,(2^{1/2})\,(2^{1/2} - 1)\,(-2^{1/2} + 1)\,(1, 2^{1/2} + 1, -1, -2^{1/2}, -2^{1/2} - 1) .$$

(b) $n = 3$.

The fifth, seventh, eighth and thirteenth powers require respectively,

$$\alpha_4 + \alpha_1\alpha_3 + \alpha_1^4 = 0 . \tag{1}$$

$$\alpha_1\alpha_5^3 + \alpha_4^4 + \alpha_1^4\alpha_4^3 + \alpha_1^3\alpha_3^3\alpha_4 = 0 . \tag{2}$$

$$\alpha_3\alpha_4\alpha_5^3 + 2\alpha_4^3\alpha_5^2 + \alpha_1^3\alpha_4\alpha_5^3 + \alpha_1\alpha_3^3\alpha_4^3 + 2\alpha_3^6\alpha_4 + \alpha_1^4\alpha_3\alpha_5^3 + 2\alpha_1^3\alpha_3^3\alpha_5^2 + \alpha_1^3\alpha_3\alpha_4^4 + 2\alpha_1\alpha_3^7 = 0 . \tag{3}$$

$$1 + \alpha_1^9\alpha_4^3\alpha_5 + \alpha_1^3\alpha_4\alpha_5^9 + \alpha_1\alpha_4^9\alpha_5^3 + \alpha_4^{13} = 0 . \tag{4}$$

The tenth power gives an identity; the eleventh requires exactly the 9th power of (2).

Applying (1) to (2)

$$\alpha_1(\alpha_5^3 + 2\alpha_1^6\alpha_3^3 + \alpha_1^{12}\alpha_3) = 0$$

or

$$\alpha_5 = \alpha_1^2\alpha_3 + 2\alpha_1^4\alpha_3^9 . \tag{5}$$

(b_1) If $\alpha_3 = 0$, then $\alpha_5 = 0$, $\alpha_4 = -\alpha_1^4$ and the sextic obtained, $\xi^6 + \alpha_1\xi^5 - \alpha_1^4\xi^2$ is suitable on the mark of the $GF[3^3]$. Thus $\xi^6 + \xi^5 - \xi^2$ represents the substitution

$$(0)\,(1)\,(-1)\,(j, j^2 - 1, -j^2 + j - 1, -j^2 + j + 1, j - 1, j^2 + j, -j^2, -j^2 - 1, j + 1, j^2 - j, -j^2 - j - 1, -j^2 - j + 1)\,(-j, -j^2 + j, j^2, j^2 + j - 1, -j - 1, -j^2 - j, j^2 - j + 1, j^2 + 1, -j + 1, -j^2 + 1, j^2 + j + 1, j^2 - j - 1) ,$$

where $j^3 = j + 1$ is the irreducible equation defining the $GF[3^3]$.

(b_2) If $a_3 \neq 0$, we have on applying (1) and (5) to (3),

$$a_1^{13}a_3(2a_1^6 + 2a_3^2 + a_1^5a_3^9 + a_1^7a_3^{17}) = 0 .$$

Writing $a_3 = \eta a_1^3$, this becomes

$$\eta^{17} + \eta^9 - \eta^2 - 1 = 0 .$$

Multiply by η^9, replace η^{11} by η^{11+52} and η^{26} by 1 :

$$1 + \eta^{18} - \eta^{63} - \eta^9 = 0 .$$

Extracting the ninth root,

$$1 + \eta^2 - \eta^7 - \eta = -(\eta - 1)^2(\eta^2 + 1)(\eta^3 - \eta^2 - \eta - 1) = 0 .$$

Now $\eta = 1$ is excluded since $\xi^6 + a_1\xi^5 + a_1^3\xi^3 + a_1^4\xi^2$ vanishes for $\xi = -a_1$.
Again $\eta^2 \neq -1$, since then $\eta^{26} = -1$.
If $\eta^3 = \eta^2 + \eta + 1$, then $\eta^9 = -\eta^2 + \eta$, $\eta^{13} = 1$.
From (1) and (5)

$$a_3 = \eta a_1^3, \quad a_4 = -(\eta + 1)a_1^4, \quad a_5 = (\eta + 2\eta^9)a_1^5 = \eta^2 a_1^5 .$$

Substituting these values in (4), using $\eta^{13} = 1$, we have

$$-\eta^{12} - \eta^{10} - \eta^9 + \eta^6 + \eta^5 - \eta^4 - \eta^3 + \eta^2 - \eta - 1 = 0 .$$

which is readily seen to be inconsistent with

$$\eta^3 = \eta^2 + \eta + 1 .$$

(c) $n > 3$. Write $3^n = 6m + 3$.
The powers $m + 1$ and $m + 2$ require respectively,

$$a_4 + a_1a_3 + a_1^4 = 0$$

$$a_1a_5^3 + a_4^4 + a_1^4a_4^3 + a_1^3a_3^3a_4 + a_1^{12}a_4 + 2a_1^{16} = 0 .$$

From these

$$a_1(a_5^3 + 2a_1^6a_3^3 + a_1^{15}) = 0$$

or

$$a_5 = a_1^2a_3 + 2a_1^5 .$$

But

$$\xi^6 + a_1\xi^5 + a_3\xi^3 - (a_1a_3 + a_1^4)\xi^2 + (a_1^2a_3 + 2a_1^5)\xi$$

vanishes for $\xi = -a_1$ and is thus excluded.

82. Summary of §§ 79–81. The only reduced SQ $[6 ; 3^n]$ are the last five quantics in the table § 87.

Introductory study of sextics on 2^n letters, §§ 83.

83. If $\varphi(\xi) \equiv \xi^6 + a_1\xi^5 + a_2\xi^4 + a_3\xi^3 + a_4\xi^2 + a_5\xi$, then

$$\varphi(\xi+\eta) = \xi^6 + a_1\xi^5 + (\eta^2 + a_1\eta + a_2)\,\xi^4 + a_3\xi^3 + (\eta^4 + a_3\eta + a_4)\,\xi^2 + (a_1\eta^4 + a_3\eta^2 + a_5)\,\xi + \varphi(\eta)$$

Hence in general no term can be removed. If $a_1 = 0$ we can make the coefficient of ξ^4 zero; if $a_3 = 0$, we can make that of ξ^2 zero.

84. The case n even. Then $2^n = 6m + 4$.

(a) $n = 4$. Of the "power conditions," two are independent,

$$a_3 = a_1^3 \neq 0\,.$$

$$a_2a_5^2 + a_4^3 + a_3^4 + a_2^4a_4 + a_1^4a_4^2 + a_2^6 + a_1^4a_2^2a_4 + a_1^4a_2a_3^2 + a_1^2a_2^5 + a_1^2a_5^5 + a_1a_3^2a_5^4 + a_1a_4^4a_5^2 + a_2^2a_3a_5^4 + a_3^4a_5^3 + a_3^2a_4^4a_5 + a_3a_4^6 = 0\,.$$

(b) $n > 4$.

The power $m + 1$ requires $a_3 = a_1^3$. Applying this to the condition given by the power $m + 5$:

$$a_1^2a_5^5 + a_1^7a_5^4 + a_1^3a_2^2a_5^4 + a_1a_4^4a_5^2 + a_1a_2^8a_5^2 + a_1^9a_2^4a_5^2 + a_1^6a_4^4a_5 + a_1^{22}a_5 + a_1^{14}a_2^4a_5 + a_1^3a_4^6 + a_1^3a_2^8a_4^2 + a_1^{27} + a_1^{11}a_2^4a_4^2 + a_1^{23}a_2^2 + a_1^{11}a_2^8 + a_1^7a_2^{10} = 0\,.$$

By the method of proof used in (f) § 73, we find the power

$$2m + 1 = 2^{n-2} + 2^{n-4} + \ldots + 2^2 + 1$$

requires

$$1 + a_3^{2m+1} = 0 \text{ or } a_3 \neq 0\,.$$

85. The case n odd. Then $2^n = 6m + 2$.

(a) $n = 3$. The third power requires

$$a_4 + a_2^2 + a_1^2a_2 + a_1a_5^2 + a_3^2a_5 + a_3a_4^2 = 0\,. \tag{13}$$

The fifth power requires exactly the 4th power of this.

(b) $n > 3$. The power $m + 2$ requires

$$a_1a_5^2 + a_3a_4^2 + a_3^2a_5 + a_2^4a_3 + a_1^6a_5 + a_1^5a_3^2 + a_1^4a_2^2a_3 + a_1^3a_2^4 = 0\,. \tag{1_3}$$

The power $m + 6$ requires for $n > 5$ and $n = 5$ respectively

$$(a_3 + a_1^3)(a_1^{16}a_2^8 + a_2^{16} + a_4^8) + (a_3^8 + a_1^{24})(a_1a_5^2 + a_3a_4^2 + a_3^2a_5) = 0\,. \tag{2}$$

$$a_4 + a_2^2 + a_1^2a_2 + a_4^8(a_3 + a_1^3) + a_3^8(a_1a_5^2 + a_3a_4^2 + a_3^2a_5) = 0\,. \tag{2_5}$$

The powers $m + 8$ and $m + 18$ lead to (1).

(b_1) Suppose $a_1 = 0$, so that by § 83 we can take $a_2 = 0$.

If $a_3 \neq 0$ and $n > 5$, then by (1) and (2) we find $a_4 = a_5 = 0$.

But $\xi^6 + a_3\xi^3$ vanishes for $\xi = a_3^{1/3}$; while every mark in the $GF[2^n]$, n odd, is a cube by § 18.

If $a_3 \neq 0$, and $n = 5$, (1) and (2_5) give

$$a_4^2 = a_3 a_5\,;\quad a_4 = a_3^5 a_5^4\,.$$

Thus either $a_4 = a_5 = 0$, or $a_5 = a_3^{12}$, $a_4 = a_3^{22}$.

But $\xi^6 + a_3\xi^3 + a_3^{22}\xi^2 + a_3^{12}\xi$ vanishes for $\xi = a_3^{21} = a_3^{13}$.

If $a_3 = 0$, then the power $2m + 1 = 2^{n-2} + 2^{n-4} + \ldots + 2^3 + 2 + 1$ requires $a_4 = 0$. But $\xi^6 + a_5\xi$ vanishes for $\xi = a_5^{1/5}$, a mark of the $GF[2\ ]$, n odd.

Hence every suitable sextic on 2^n letters, n odd and 73, in which the coefficient of ξ^5 is zero, is reducible to the form ξ^6.

(b_2) Suppose $a_3 = 0$, $a_1 \neq 0$. Then we may take $a_5 = 0$. Then $a_2 = 0$ by (1). For $n > 5$, $a_4 = 0$ by (2); for $n = 5$, (2_5) gives

$$a_4 + a_1^3 a_4^8 = 0\,,$$

hence either $a_4 = 0$ or $a_4 = a_1^4$.

But $\xi^6 + a_1\xi^5$ vanishes for $\xi = a_1$ and is excluded.

The sextic $\xi^6 + a_1\xi^5 + a_1^4\xi^2$ represents a substitution on the marks of the $GF[2^5]$, viz, for $a_1 = 1$:

$$\begin{aligned}(0)\ (1)\ &(j+1, j^3+j^2, j^2+1, j^4+j^3+j, j^4+1)\,(j^3+j, j^4+j^3+1,\\ &j^4+j+1, j^4+j^3+j^2+1)\,(j^3, j^4+j^2+j, j^4+j^3+j^2+j, j^4+j^2,\\ &j^3+j^2+j, j^2+j)\,(j, j^3+j+1, j^4+j^3+j^2, j^2, j^3+j^2+j+1,\\ &j^4+j^2+j+1, j^4, j^4+j^3+j^2+j+1, j^4+j^3, j^3+j^2+1, j^4+j,\\ &j^2+j+1, j^4+j^3+j+1, j^3+1, j^4+j^2+1)\,,\end{aligned}$$

the $GF[2^5]$ being defined by the equation $j^5 = j^2 + 1$.

(b_3) Suppose $a_3 = a_1^3 \neq 0$. Then by (1)

$$a_5 = a_1^5 + a_1^3 a_2 + a_1 a_4\,.$$

(2) and (2_5) and (1_3) are seen to be satisfied; but

$$\xi^6 + a_1\xi^5 + a_2\xi^4 + a_1^3\xi^3 + a_4\xi^2 + (a_1^5 + a_1^3 a_2 + a_1 a_4)\,\xi$$

vanishes for $\xi = a_1$.

86. Summary of §§ 83–85. If a sextic represent a substitution on the marks of the $GF[2^n]$, then, for n even,

$$a_3 = a_1^3 \neq 0\,;$$

for n odd and > 3,

$$a_1 \neq 0\,,\quad a_3 \neq 0\,,\quad a_3 \neq a_1^3\,,$$

except for the suitable quantics

$$\xi^6 \text{ on } 2^n \text{ letters}\,;\quad \xi^6 + a\xi^5 + a^4\xi^2 \text{ on } 2^5 \text{ letters.}$$

87. *Table.**

Except for sextics on 2^n letters, the following is a complete list of all *reduced* quantics $\varphi(\xi)$ of degree $\leqq 6$ which are suitable to represent substitutions on a power of a prime number of letters. From them (by § 16) all suitable quantics whatsoever of degree $\leqq 6$ are obtained by the formula

$$a\varphi(\xi + \beta) + \gamma .$$

Reduced quantic.	Suitable for $p^n =$
ξ	any
ξ^2	2^n
ξ^3	3^n, $3m + 2$
$\xi^3 - a\xi$ (a = not-square)	3^n
$\xi^4 \pm 3\xi$	7
$\xi^4 + a_2\xi^2 + a_3\xi$ (when it vanishes only for $\xi = 0$)	2^n
ξ^5	5^n, $5m \pm 2$, $5m + 4$
$\xi^5 - a\xi$ (a = not 4th power)	5^n
$\xi^5 + 2^{1/2}\xi$	3^2
$\xi^5 \pm 2\xi^2$	7
$\xi^5 + a\xi^3 \pm \xi^2 + 3a^2\xi$ (a = not-square)	7
$5\xi^2 + 5a\xi^3 + a^2\xi$ (a = arbitrary)	$5m \pm 2$
$\xi^5 + a\xi^3 + 3a^2\xi$ (a = not-square)	13
$\xi^5 + 2a\xi^3 + a^2\xi$ (a = not-square)	5^n
ξ^6	2^n, n odd.
$\xi^6 \pm 2\xi$	11
$\xi^6 \pm a^2\xi^3 + a\xi^2 \pm 5\xi$ (a = square)	11
$\xi^6 \pm 4a^2\xi^3 + a\xi^2 \pm 4\xi$ (a = 0 or not-square)	11
$\xi^6 + a_2\xi^4 + a_3\xi^3 + a_2^2\xi_2 + (2a_2a_3 \pm a_2^{5/2})\xi$ (a_2 = square $\neq 0$; $a_3 = 0$, $\pm 2^{1/2}a_2^{3/2}$, $\pm a_2^{3/2}$, or $\pm (2^{1/2} + 1)\, a_2^{3/2}$, the signs to correspond to that of $\pm a_2^{5/2}$).	3^2
$\xi^6 + a\xi^5 - a^4\xi^2$ (a = arbitrary)	3^3, 2^5
$\xi^6 + a\xi^5 + a^3\xi^3 - a^4\xi^2 - a^5\xi$ (a = arbitrary)	3^2
$\xi^6 + a\xi^5 + \varphi a^3\xi^3 - \varphi a^4\xi^2 + 2^{1/2}a^5\xi$ (a = arbitrary) (where $\varphi = \pm(1 - 2^{1/2})$).	3^2
$\xi^6 + a\xi^5 - a^3\xi^3 + a^4\xi^2 + (2^{1/2} - 1)\, a^5\xi$ (a = arbitrary)	3^2

In this table $2^{1/2}$ occurs always as a symbol for *either* of the two marks of the $GF[3^2]$ satisfying the equation $x^2 - 2 = 0$.

88. Theorem. *All substitutions on 7 letters may be derived from the two*

$$x' = ax + b\,;\quad x' = x^5\,.$$

$$\begin{pmatrix} x \\ x + b \end{pmatrix} \begin{pmatrix} x \\ x^5 + b^5 \end{pmatrix} \begin{pmatrix} x \\ 3b^4x^5 + 2b^5 \end{pmatrix} = \begin{pmatrix} x \\ x^5 - b^2x^3 + b^3x^2 + 3b^4x \end{pmatrix}; \qquad (1)$$

* Compare *American Journal of Mathematics*, vol. 18, p. 218, § 19.

so that we reach the form

$$x^5 + ax^3 \pm x^2 + 3a^2x, \quad a = \text{quadratic non-residue of } 7.$$

$$\begin{bmatrix} x \\ x - b^5 \end{bmatrix} \begin{bmatrix} x \\ x^5 \end{bmatrix} \begin{bmatrix} x \\ x^5 - b^2x^3 + b^3x^2 + 3b^4x \end{bmatrix} \begin{bmatrix} x \\ 5b^2x + 3b \end{bmatrix} = \begin{bmatrix} x \\ x^5 - b^4x^3 + 3b^2x \end{bmatrix}; \quad (2)$$

so that by writing $b = c^5$ we reach the form

$$x^5 - c^2x^3 + 3c^4x.$$

$$\begin{bmatrix} x \\ x^5 \end{bmatrix} \begin{bmatrix} x \\ x^5 - b^4x^3 + 3b^2x \end{bmatrix} \begin{bmatrix} x \\ 5b^4x \end{bmatrix} = \begin{bmatrix} x \\ x^5 + 2b^2x^3 + 3\,(2b^2)^2x \end{bmatrix}. \quad (3)$$

Hence by (1) and (2) we reach the form

$$x^5 + ax^3 + 3a^2x, \qquad a = \text{arbitrary}.$$

$$\begin{bmatrix} x \\ x + 3b^5 \end{bmatrix} \begin{bmatrix} x \\ x^5 + b \end{bmatrix} \begin{bmatrix} x \\ x^5 - b^2x^3 + b^3x^2 + 3b^4x \end{bmatrix} \begin{bmatrix} x \\ b^3x + 2b^2 \end{bmatrix} = \begin{bmatrix} x \\ x^4 + 4b^3x \end{bmatrix}; \quad (4)$$

so that we reach $x^4 \pm 3x$.

$$\begin{bmatrix} x \\ x^5 \end{bmatrix} \begin{bmatrix} x \\ x^4 + 4b^3x \end{bmatrix} \begin{bmatrix} x \\ 2b^3x \end{bmatrix} = \begin{bmatrix} x \\ x^5 + 2b^3x \end{bmatrix}; \quad (5)$$

so that we reach $x^5 \pm 2x$.

89. E. Betti proved (l. c. vol. 2, pp. 17–19, 1851) that all substitutions on 5 letters are derivable from

$$x' = ax + b\,;\ x' = x^3.$$

90. *Enumerative proof of Wilson's theorem.*

Of the $p!$ literal substitutions on a prime number p of letters, $p(p-1)$ have a linear representation

$$ax + b, \quad a \neq 0.$$

The remaining ones are represented by quantics of degree > 1 which fall into sets of $p^2(p-1)$ each, viz,

$$a\varphi(x + b) + c, \qquad a \neq 0,\ b \text{ and } c \text{ arbitrary}.$$

Hence $p! - p(p-1)$ is a multiple of $p^2(p-1)$, so that $(p-1)! + 1$ is divisible by p.

END OF PART I.